Georgia Tech Research Institute

Problem. Solved.

Scaling Interoperable Trust through a Trustmark Marketplace

John Wandelt

john.wandelt@gtri.gatech.edu

Georgia Tech Research Institute

December 2013

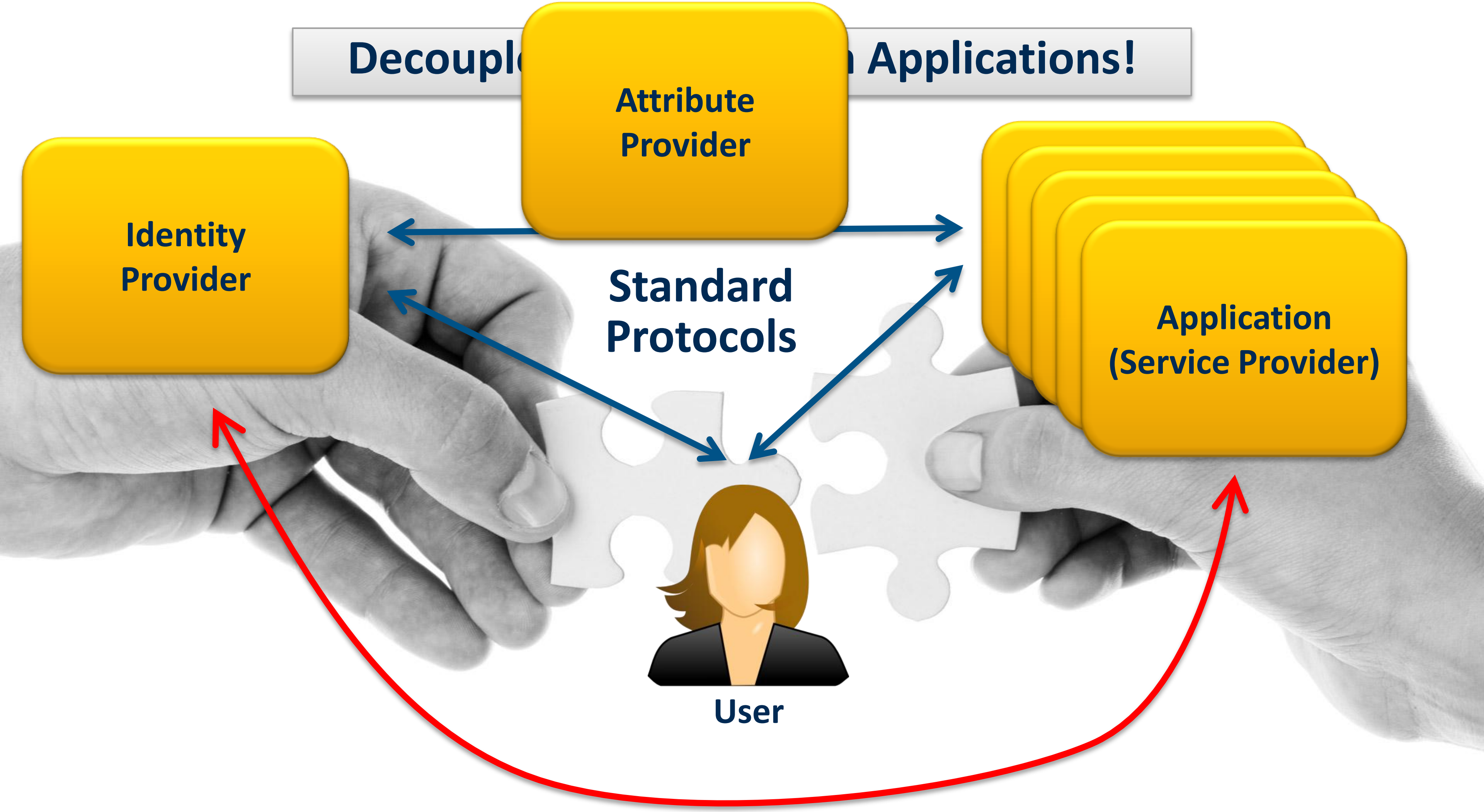
In the Beginning…

Lots of Application-Specific Identity Silos

Along Came Federated Identity…

Decoupl

Applications!



So what about **Trust, Liability, Security**?

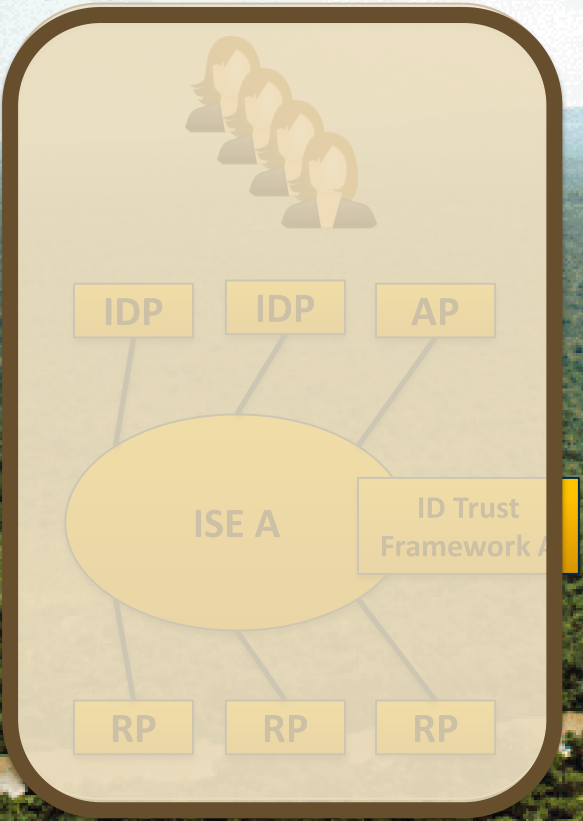
And Today…

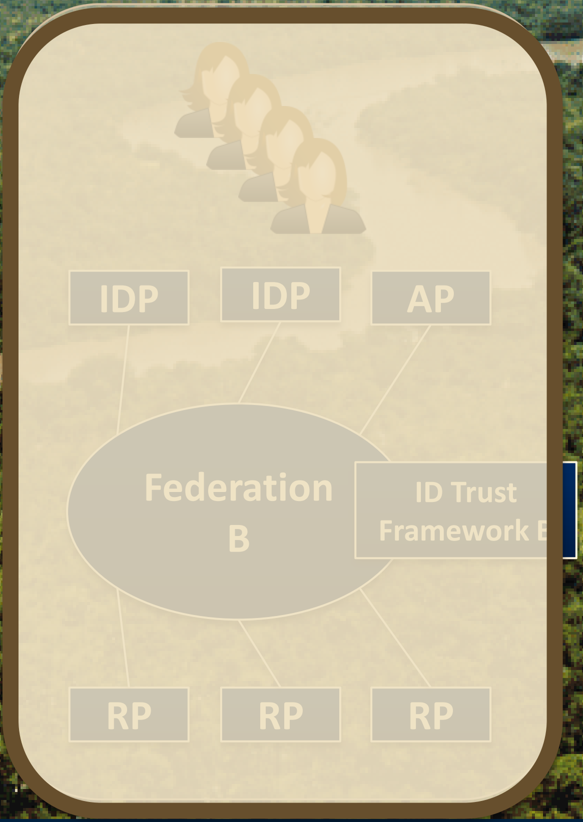
Lots of Federated Identity Silos

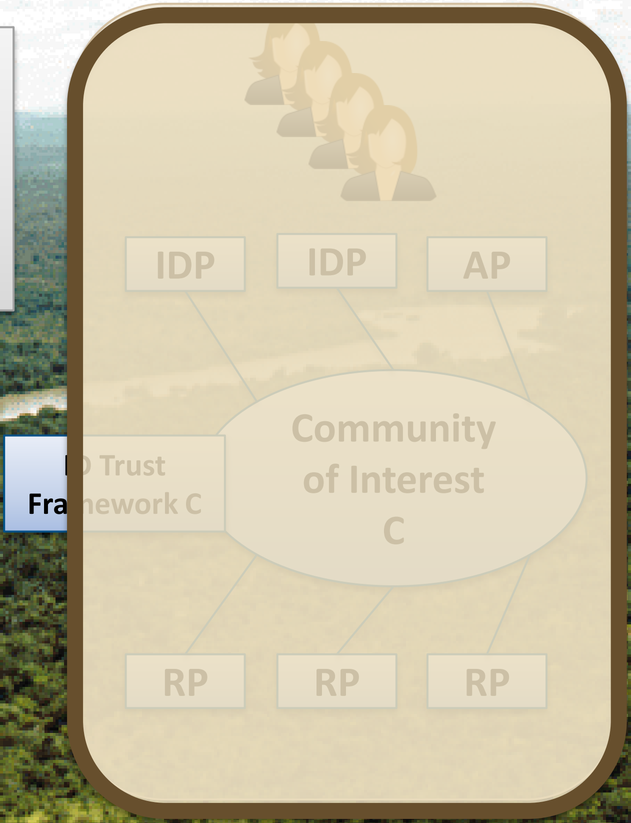
Current State of the Identity Ecosystem

Georgia Tech Research Institute

Many Trust Frameworks are **monolithic** and **opaque**.

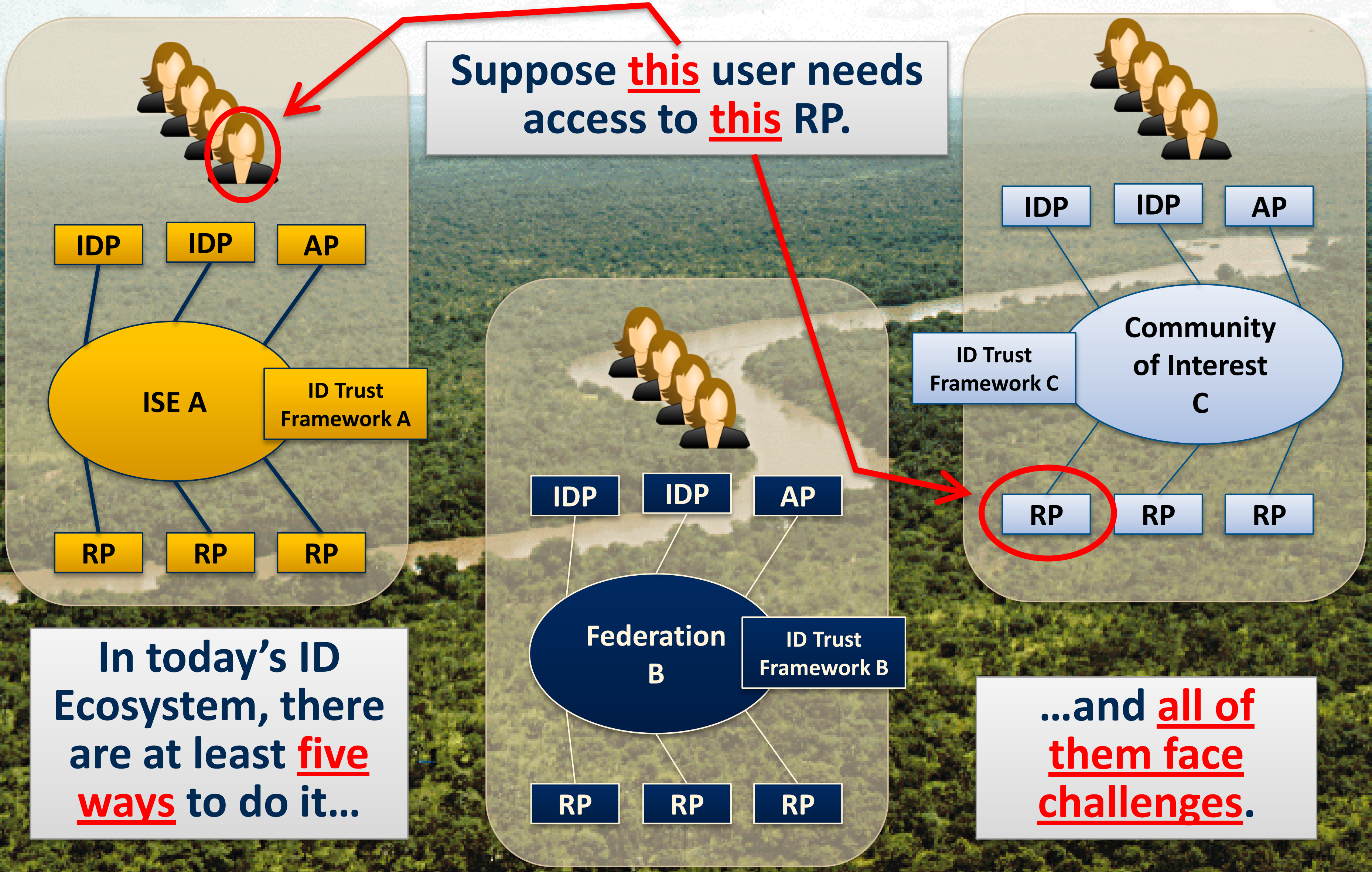






Achieving Cross-Framework Trust

Georgia Tech Research Institute



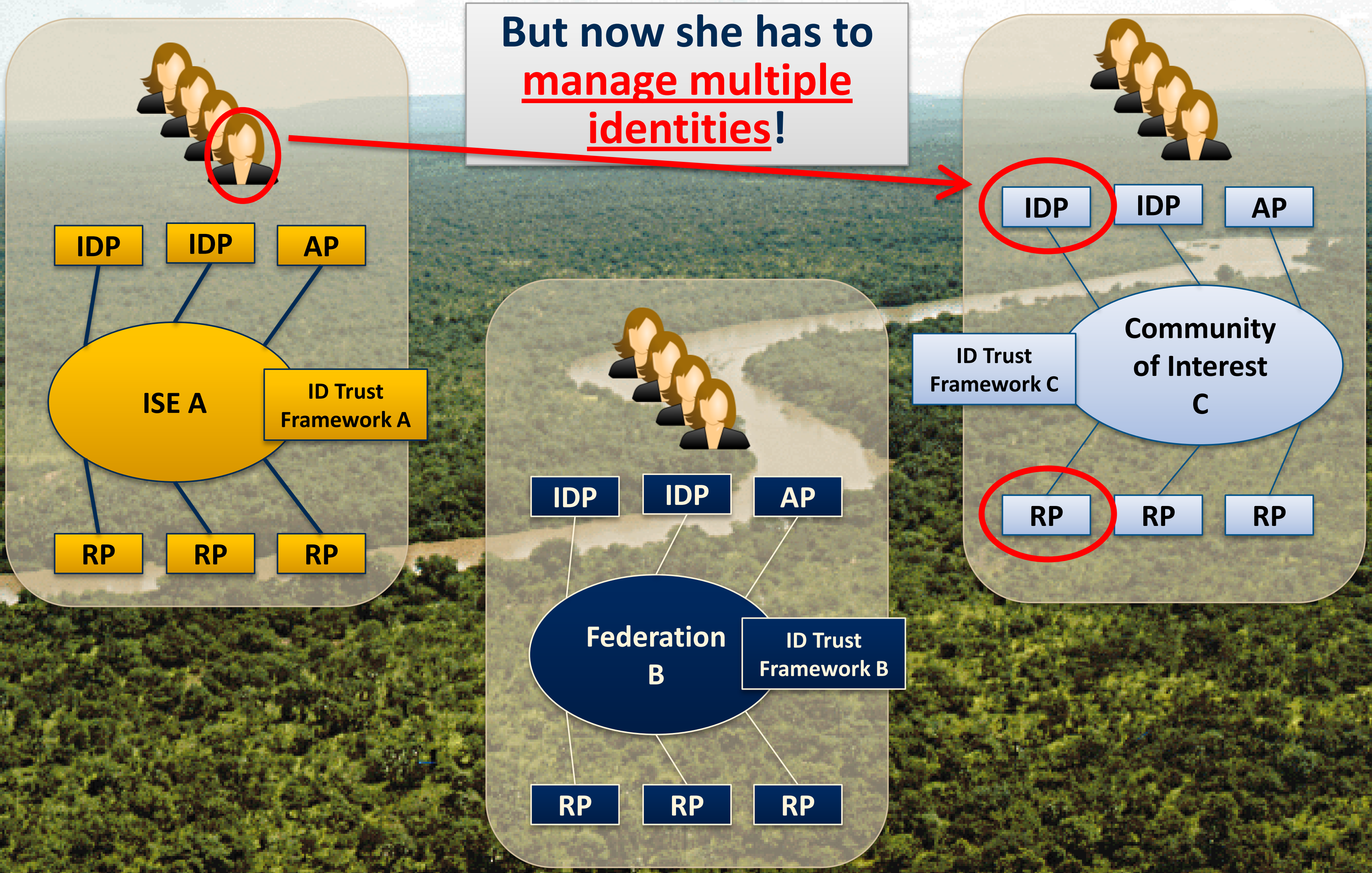
Suppose this user needs access to this RP.

In today's ID Ecosystem, there are at least five ways to do it…

…and all of them face challenges.

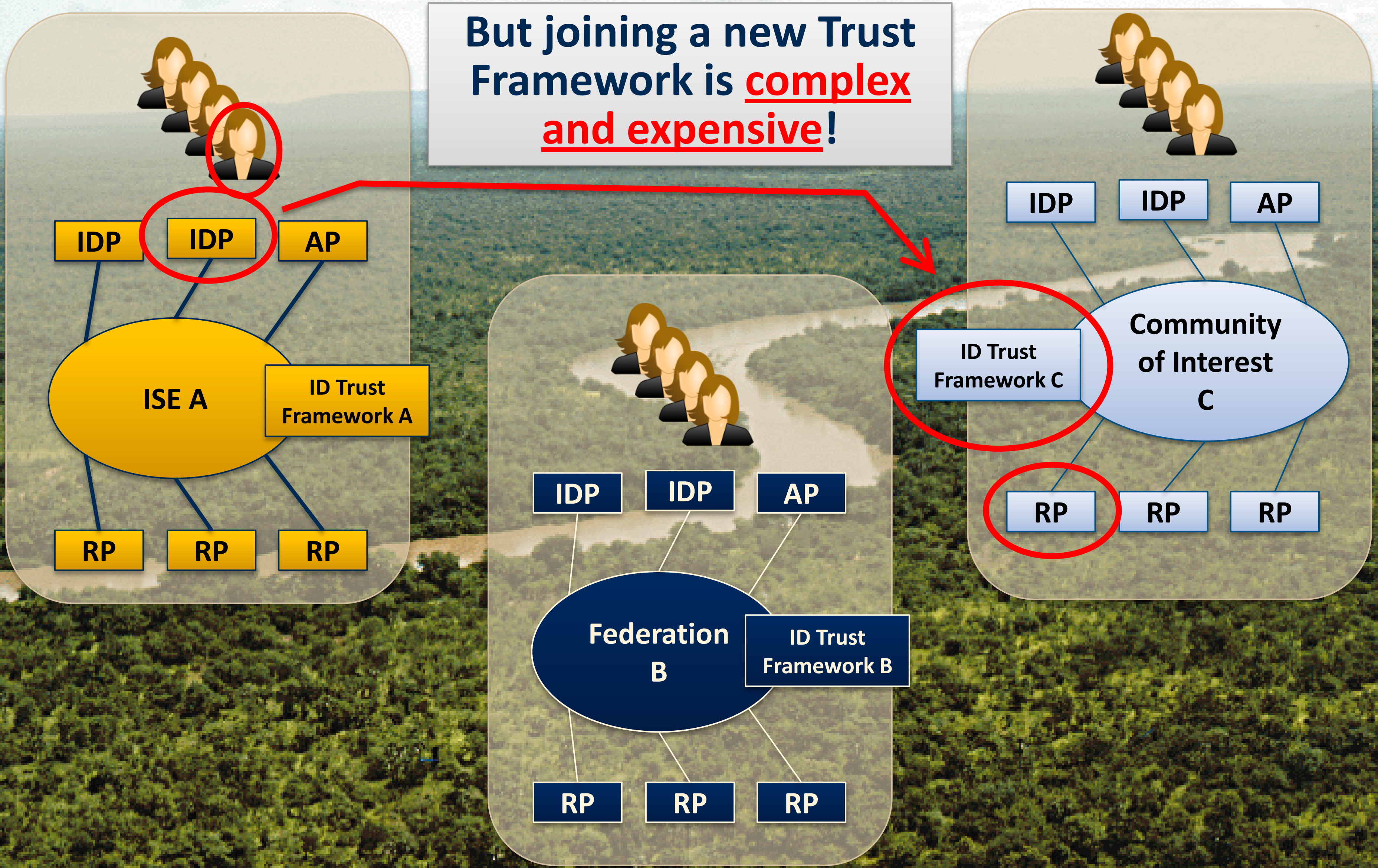
Option #1: User Creates a New Identity

But now she has to **manage multiple identities**!



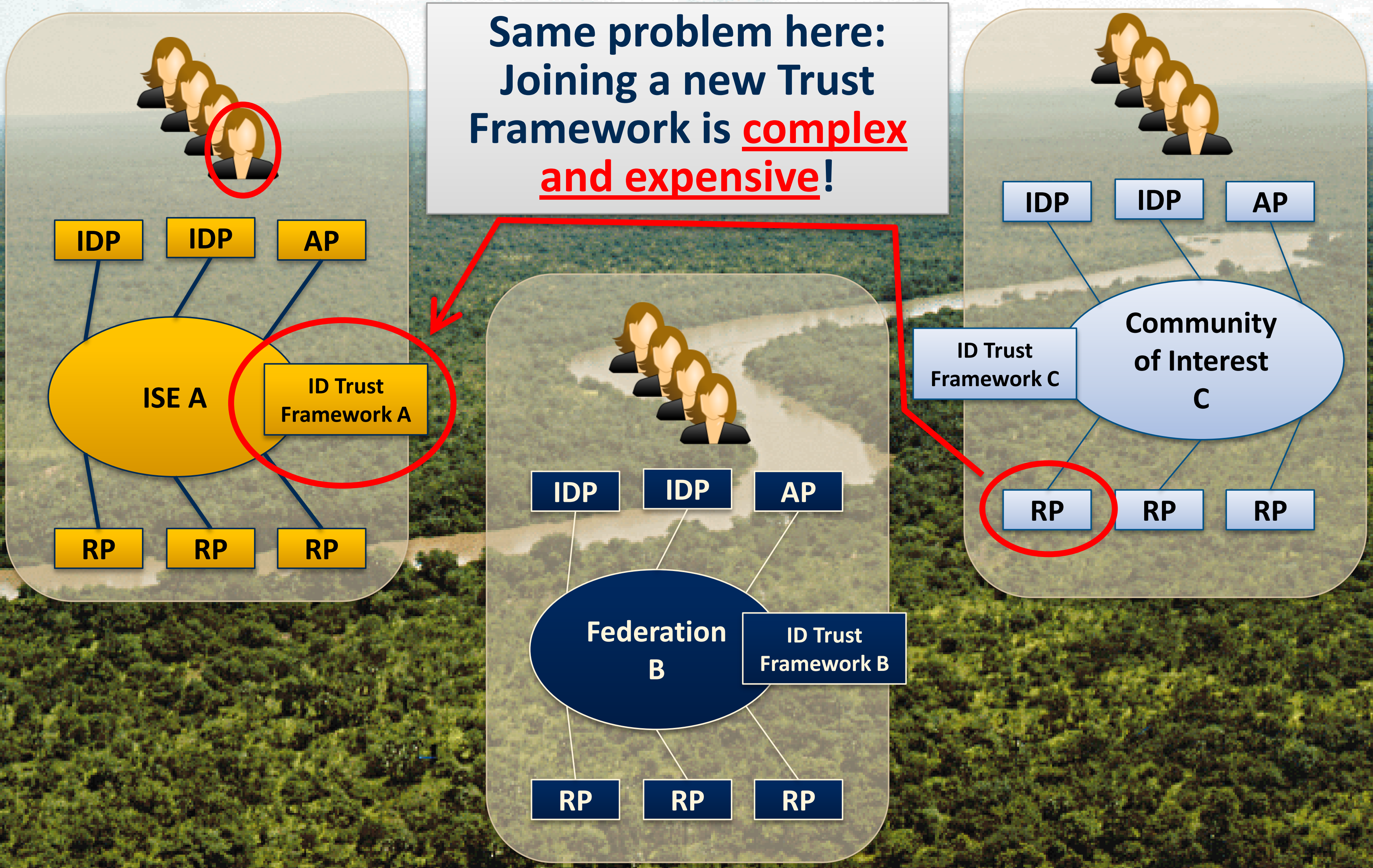
Option #2: IDP Joins New Trust Framework

But joining a new Trust Framework is **complex and expensive**!



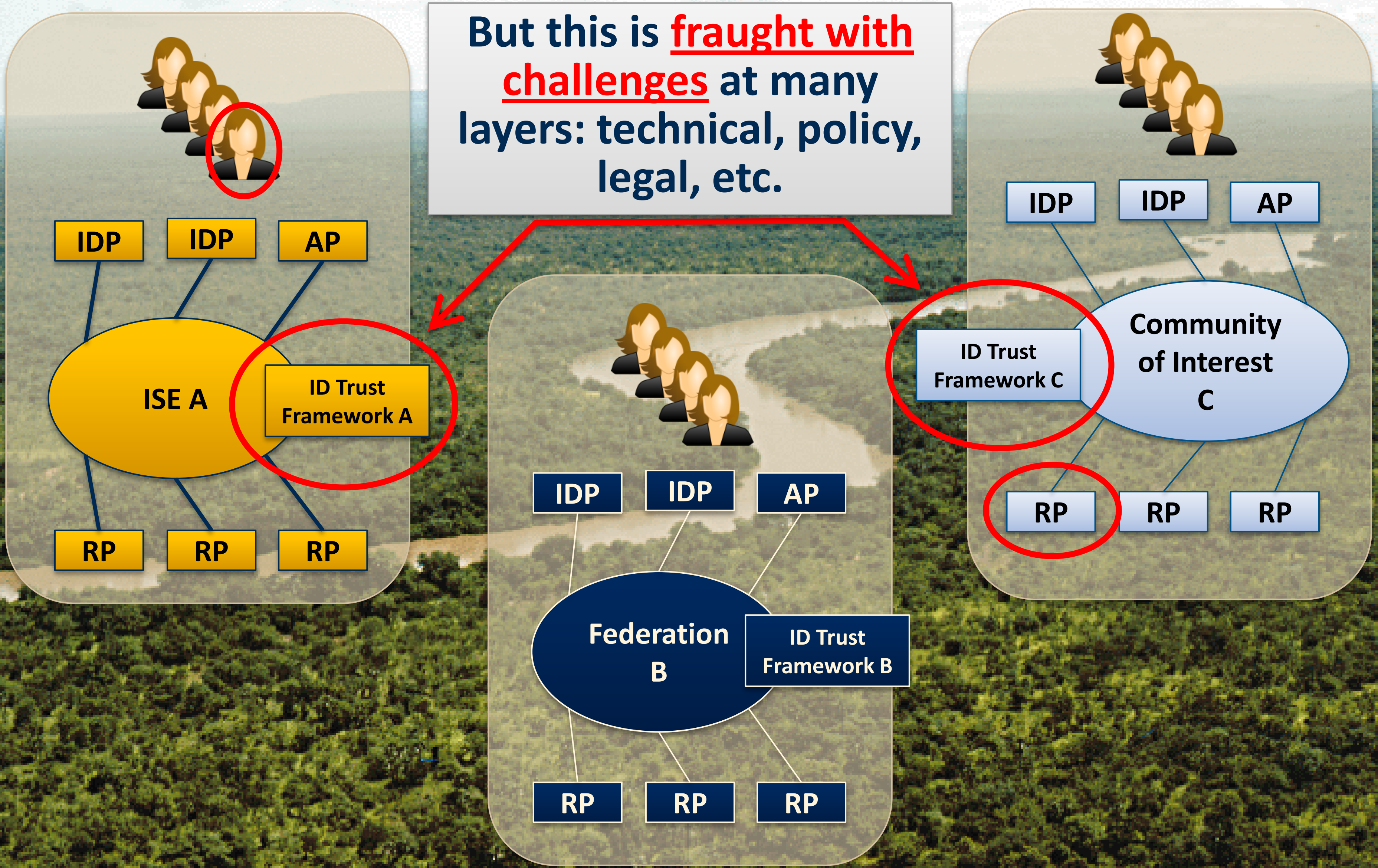
Option #3: RP Joins New Trust Framework

Same problem here: Joining a new Trust Framework is **complex and expensive**!



Option #4: Cross-Framework Relationship

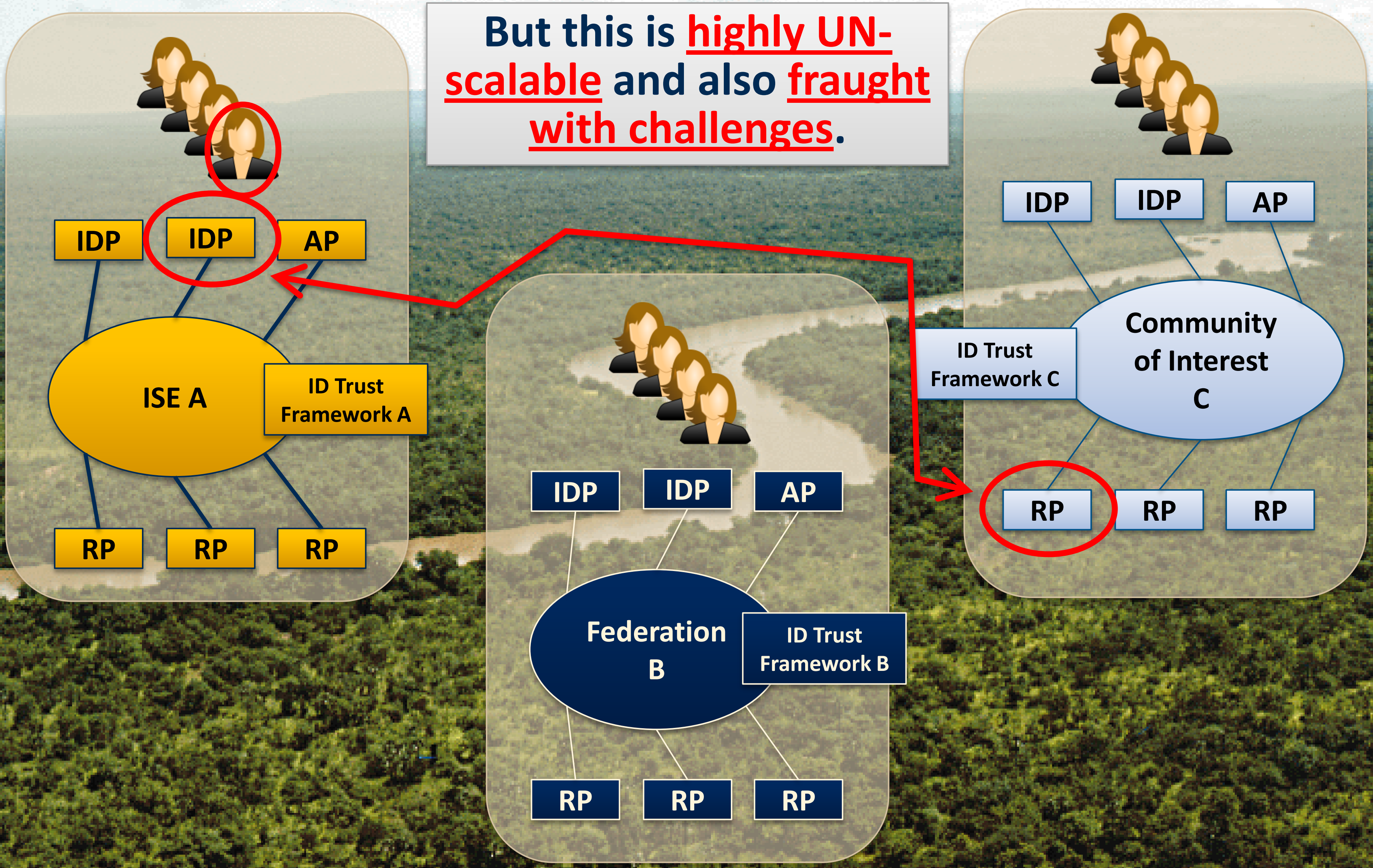
But this is **fraught with challenges** at many layers: technical, policy, legal, etc.



Option #5: Bilateral IDP-RP Relationship

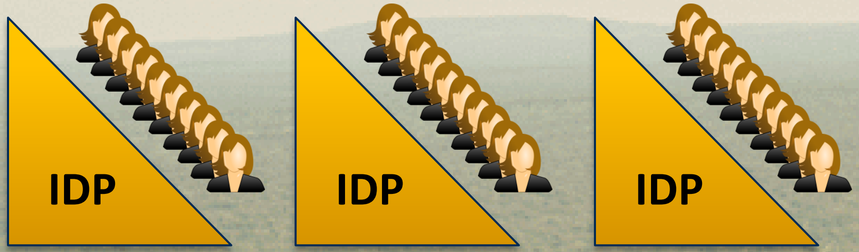
Georgia Tech Research Institute

But this is highly UN-scalable and also fraught with challenges.



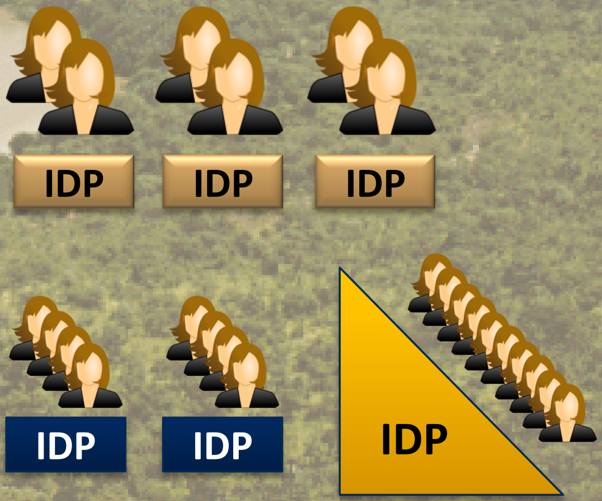
Where to from here?

A Variety of ID Ecosystem Perspectives



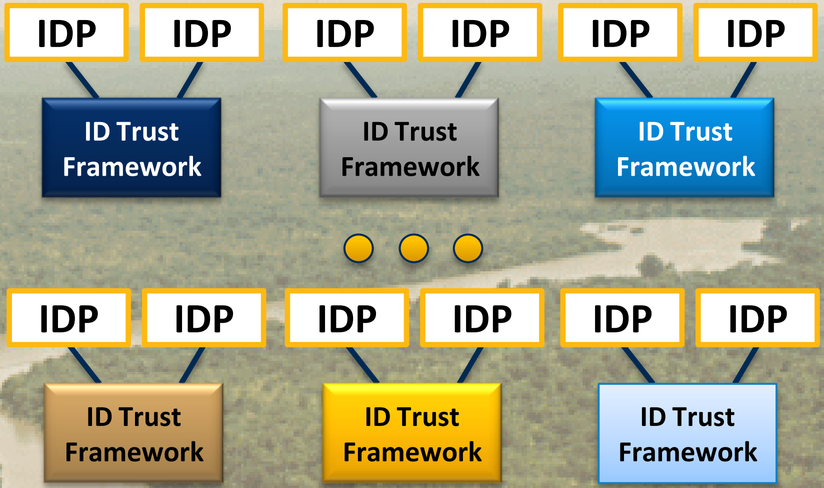
Will the ID Ecosystem have very few IDPs with consistent user bases and requirements?

Or a large number of IDPs with heterogeneous user bases and requirements?



A Variety of ID Ecosystem Perspectives

Will the ID Ecosystem have many trust frameworks with few IDPs in each?

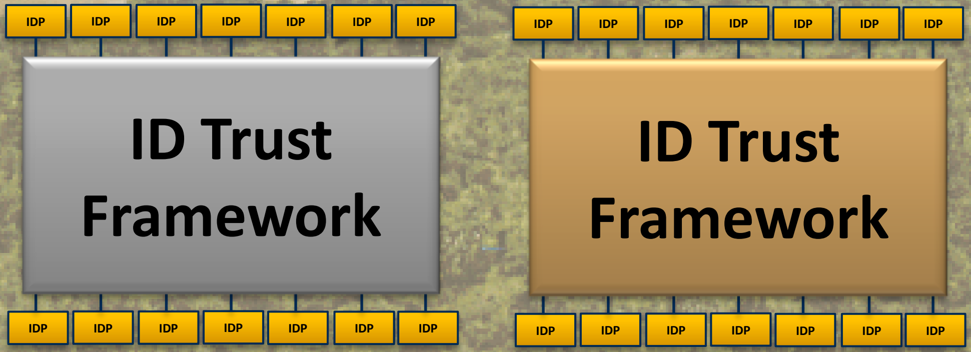


IDP IDP IDP IDP IDP IDP

ID Trust Framework
ID Trust Framework
ID Trust Framework

IDP IDP IDP IDP IDP IDP

ID Trust Framework
ID Trust Framework
ID Trust Framework



IDP IDP IDP IDP IDP IDP IDP
IDP IDP IDP IDP IDP IDP IDP

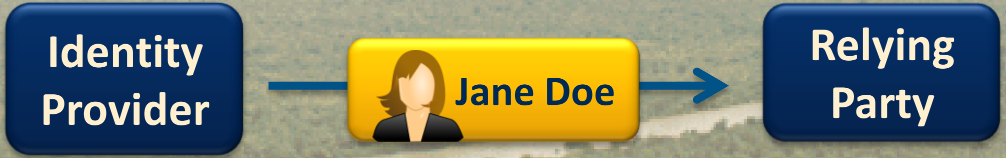
ID Trust Framework
ID Trust Framework

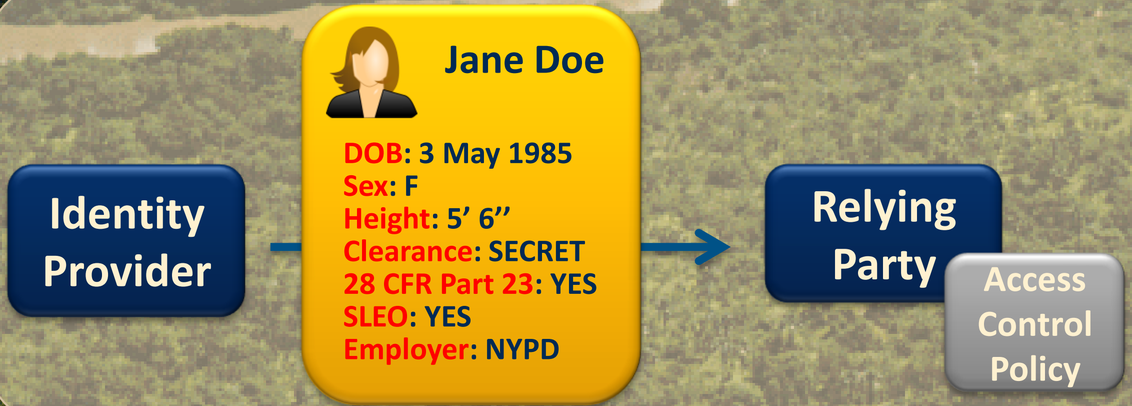
IDP IDP IDP IDP IDP IDP IDP
IDP IDP IDP IDP IDP IDP IDP

Or few trust frameworks with many IDPs in each?

A Variety of ID Ecosystem Perspectives

Is the ID Ecosystem only about identification and authentication?





DOB: 3 May 1985
Sex: F
Height: 5’ 6’’
Clearance: SECRET
28 CFR Part 23: YES
SLEO: YES
Employer: NYPD

Or are attributes and authorization fundamental to it?

ID Ecosystem Vision

Is it OK if the Trust Frameworks in the ID Ecosystem are mostly non-interoperable and non-trusting identity silos?

ID Ecosystem Vision

Or does success demand that we at least provide a viable strategy and framework for trust and interoperability between various COIs, ISEs, and Federations?

The Perspective from the LE Community

Law Enforcement COI has over 1 million people in the US alone

Over 10,000 US LE agencies

Required to share data across jurisdictions

But must obey applicable access controls when sharing

LE agencies are autonomous (NOT centrally funded)

Trust between agencies is a fundamental requirement

3rd party trust is required due to COI size and complexity

Most users must have high-assurance credentials

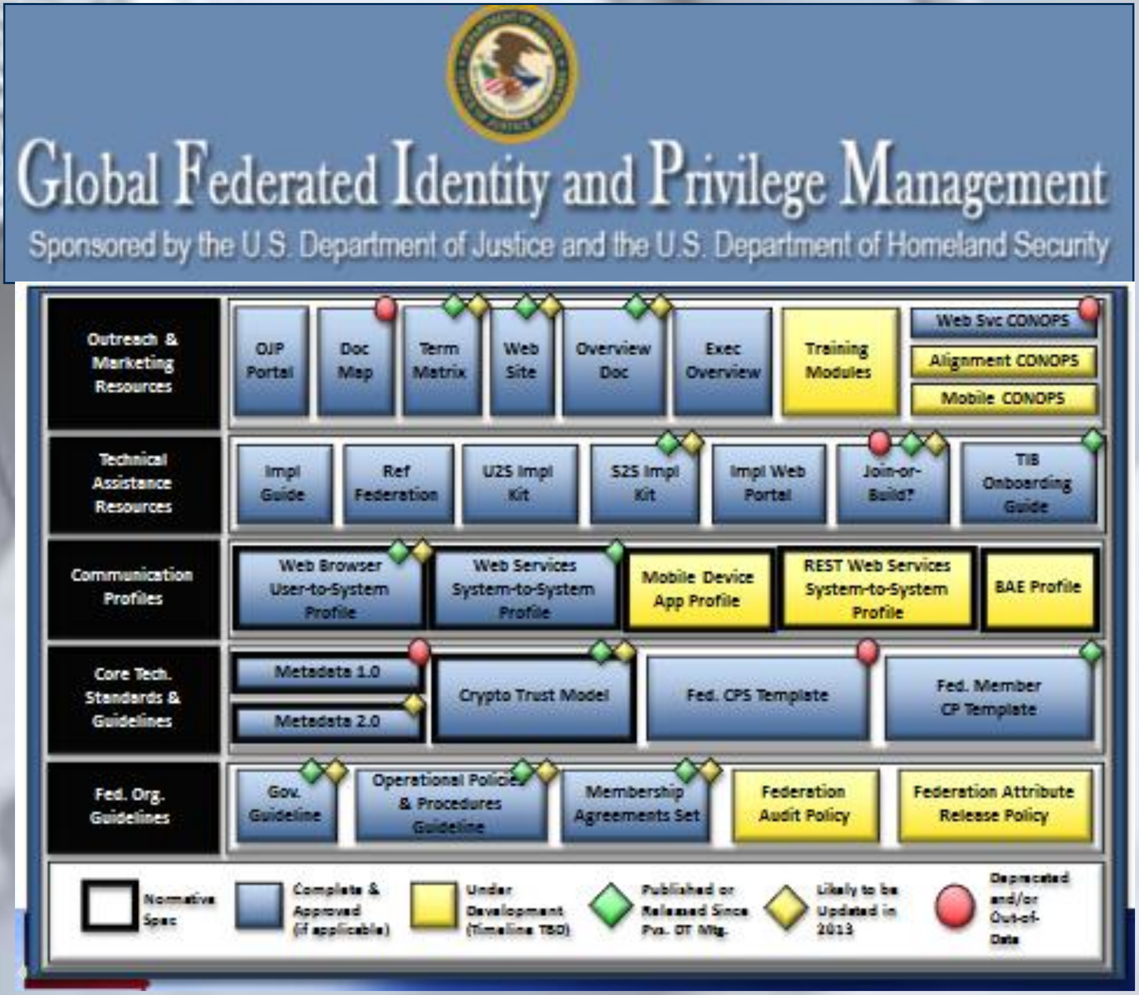
Legitimate business need to interact with many other COIs

LE agencies are highly heterogeneous

- Federal Agencies
- State Agencies
- Local Agencies
- Tribal Agencies
- Task Forces
- Fusion Centers

The Perspective from the LE Community

Georgia Tech Research Institute



Global Federated Identity and Privilege Management

Sponsored by the U.S. Department of Justice and the U.S. Department of Homeland Security

Outreach & Marketing Resources: OJP Portal; Doc Map; Term Matrix; Web Site; Overview Doc; Exec Overview; Training Modules; Web Svc CONOPS; Alignment CONOPS; Mobile CONOPS

Technical Assistance Resources: Impl Guide; Ref Federation; U2S Impl Kit; S2S Impl Kit; Impl Web Portal; Join-or-Build?; TIB Onboarding Guide

Communication Profiles: Web Browser User-to-System Profile; Web Services System-to-System Profile; Mobile Device App Profile; REST Web Services System-to-System Profile; BAE Profile

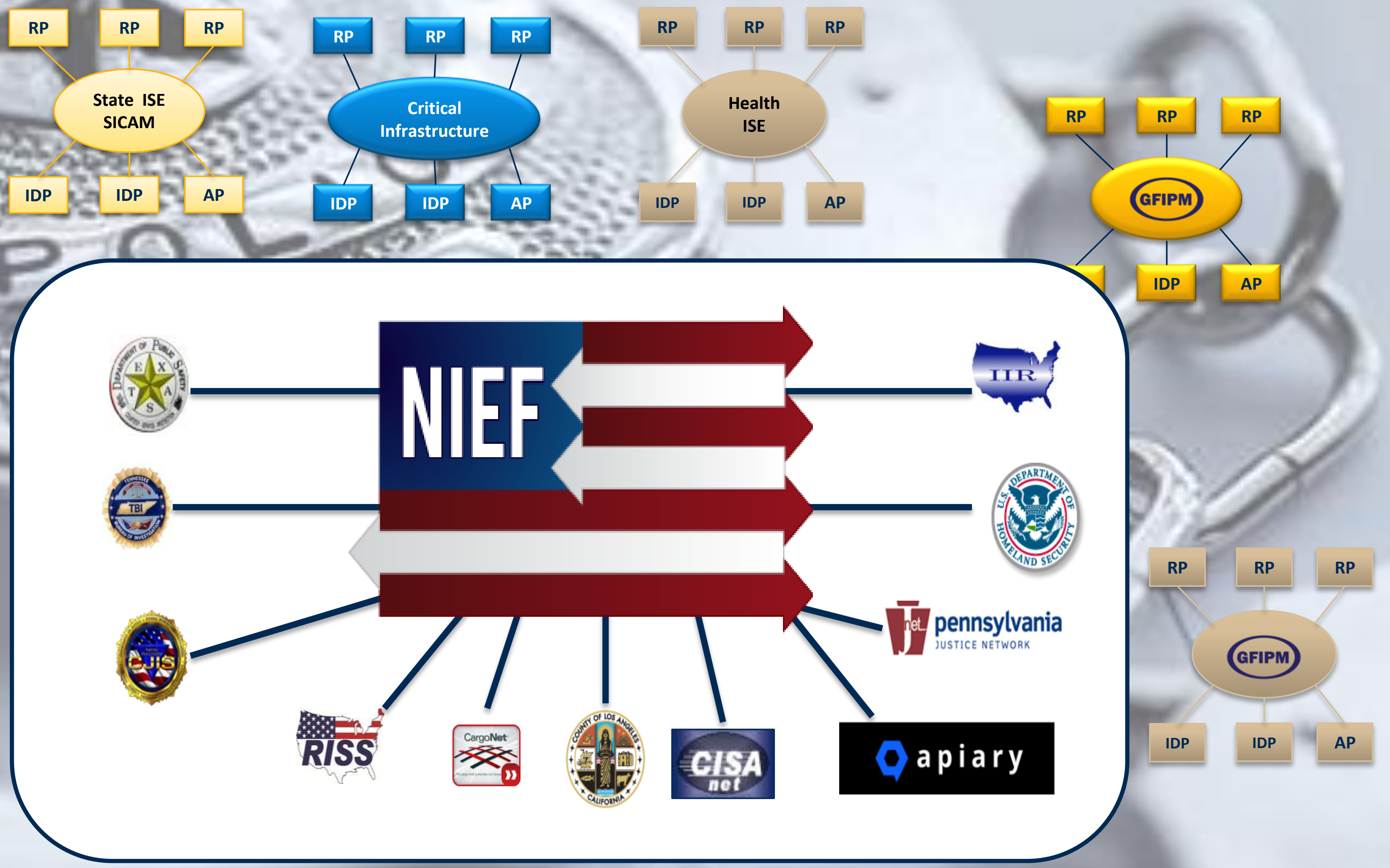
Core Tech. Standards & Guidelines: Metadata 1.0; Metadata 2.0; Crypto Trust Model; Fed. CPS Template; Fed. Member CP Template

Fed. Org. Guidelines: Gov. Guideline; Operational Policies & Procedures Guideline; Membership Agreements Set; Federation Audit Policy; Federation Attribute Release Policy

□ Normative Spec
▨ Complete & Approved (if applicable)
🟨 Under Development (Timeline TBD)
◆ Published or Released Since Pvs. OT Mtg.
◇ Likely to be Updated in 2013
● Deprecated and/or Out-of-Date

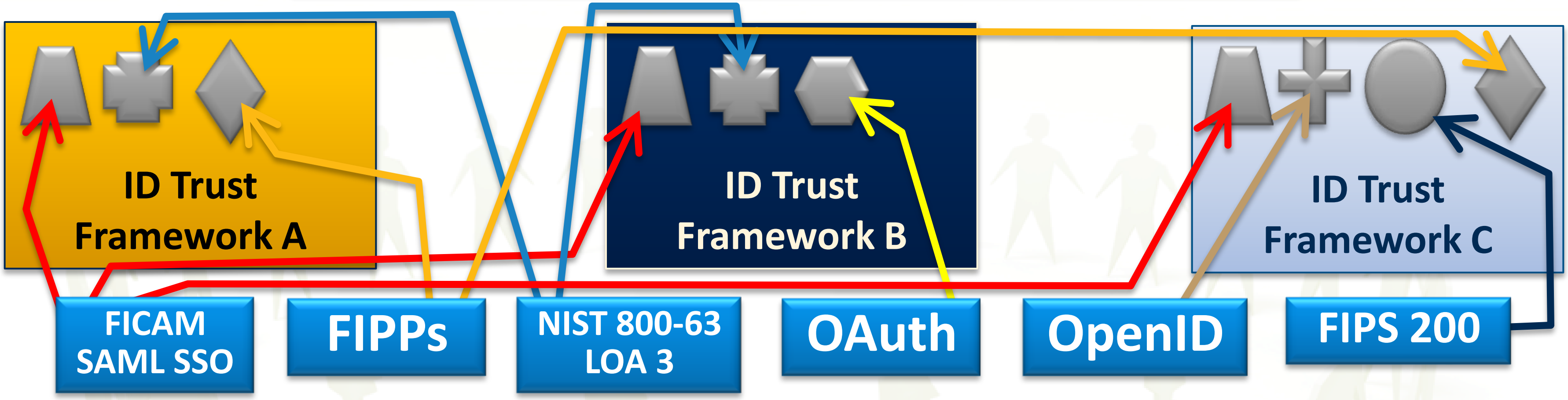
The Perspective from the LE Community

Georgia Tech Research Institute



What about a Trustmark Framework?

If the frameworks were modular…



…then we get:

Greater transparency of trust framework requirements

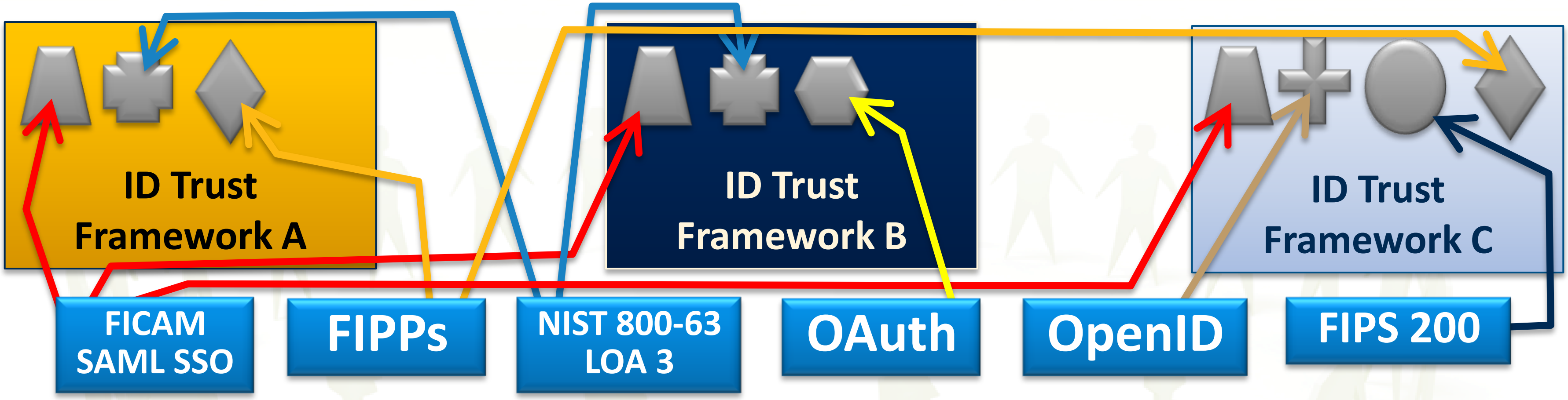
Greater ease of comparability between frameworks

Greater potential for reusability of framework components

And, most importantly:

Greater potential for participation in multiple trust frameworks by ID Ecosystem members with incremental effort and cost

What about a Trustmark Framework?



These modular components are called **Trustmarks**.

A Few Examples of Trustmarks

- FICAM SAML SSO Profile
- NIST 800-63 / FICAM LOA 3 Identity
- Fair Information Practice Principles (FIPPs)
- FIPS 200 Security Practices
- GFIPM Metadata Registry (User Attributes)

Trustmark Policies & Trustmark Agreements

Technical

Trust

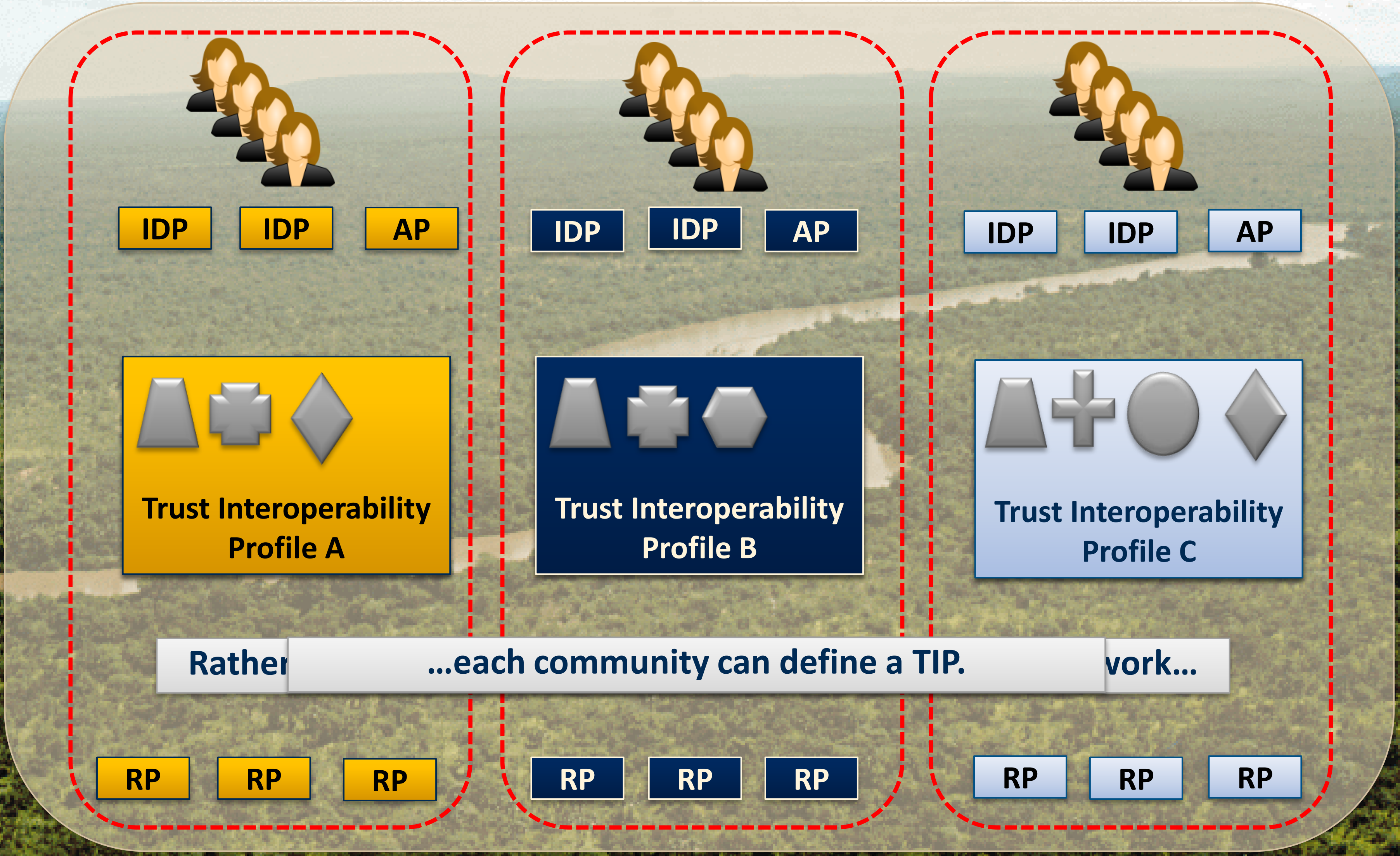
Privacy

Security

Business

Legal

A Trustmark-Based ID Ecosystem



IDP IDP AP

Trust Interoperability Profile A

RP RP RP

IDP IDP AP

Trust Interoperability Profile B

RP RP RP

IDP IDP AP

Trust Interoperability Profile C

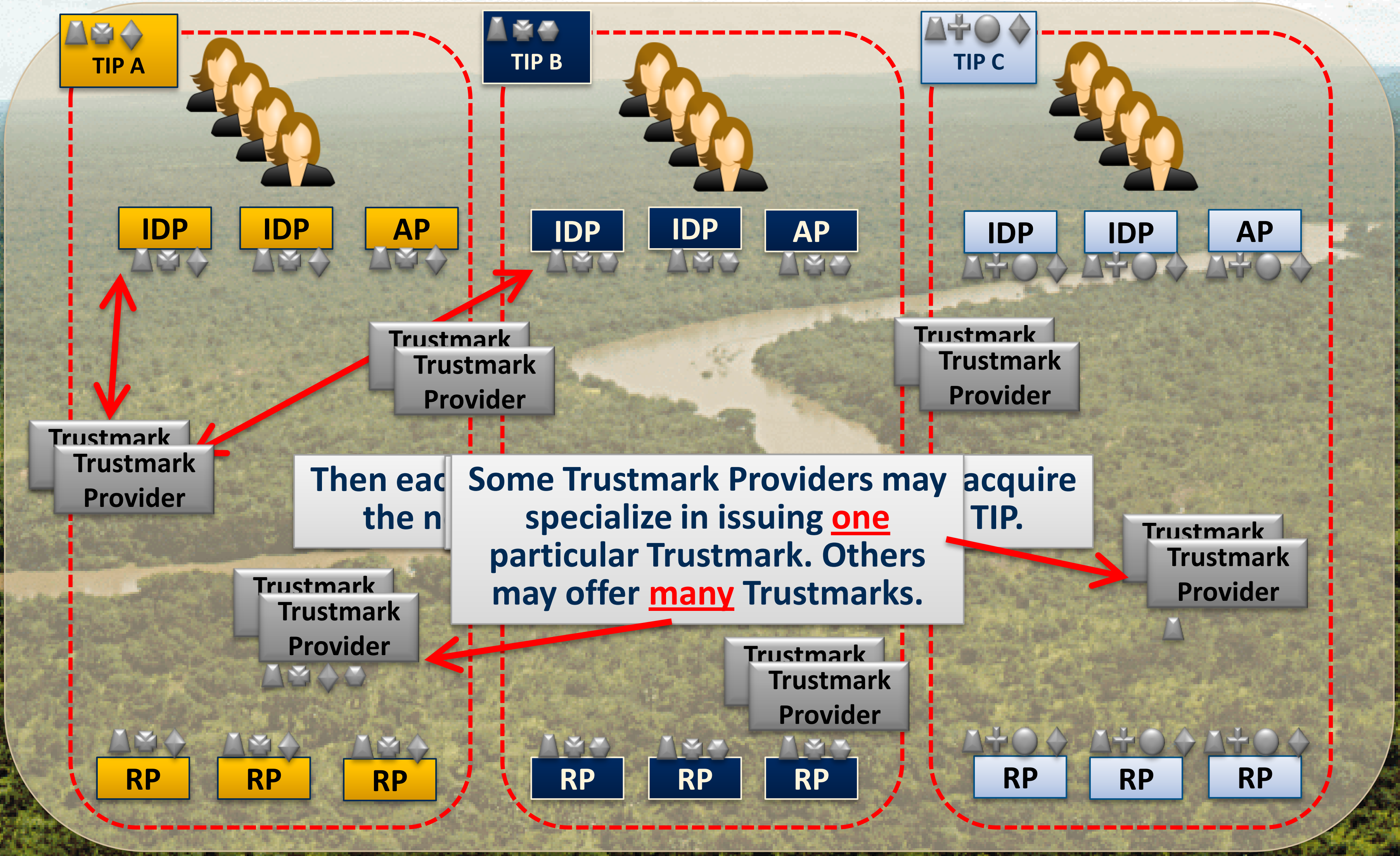
RP RP RP

Rather

…each community can define a TIP.

vork…

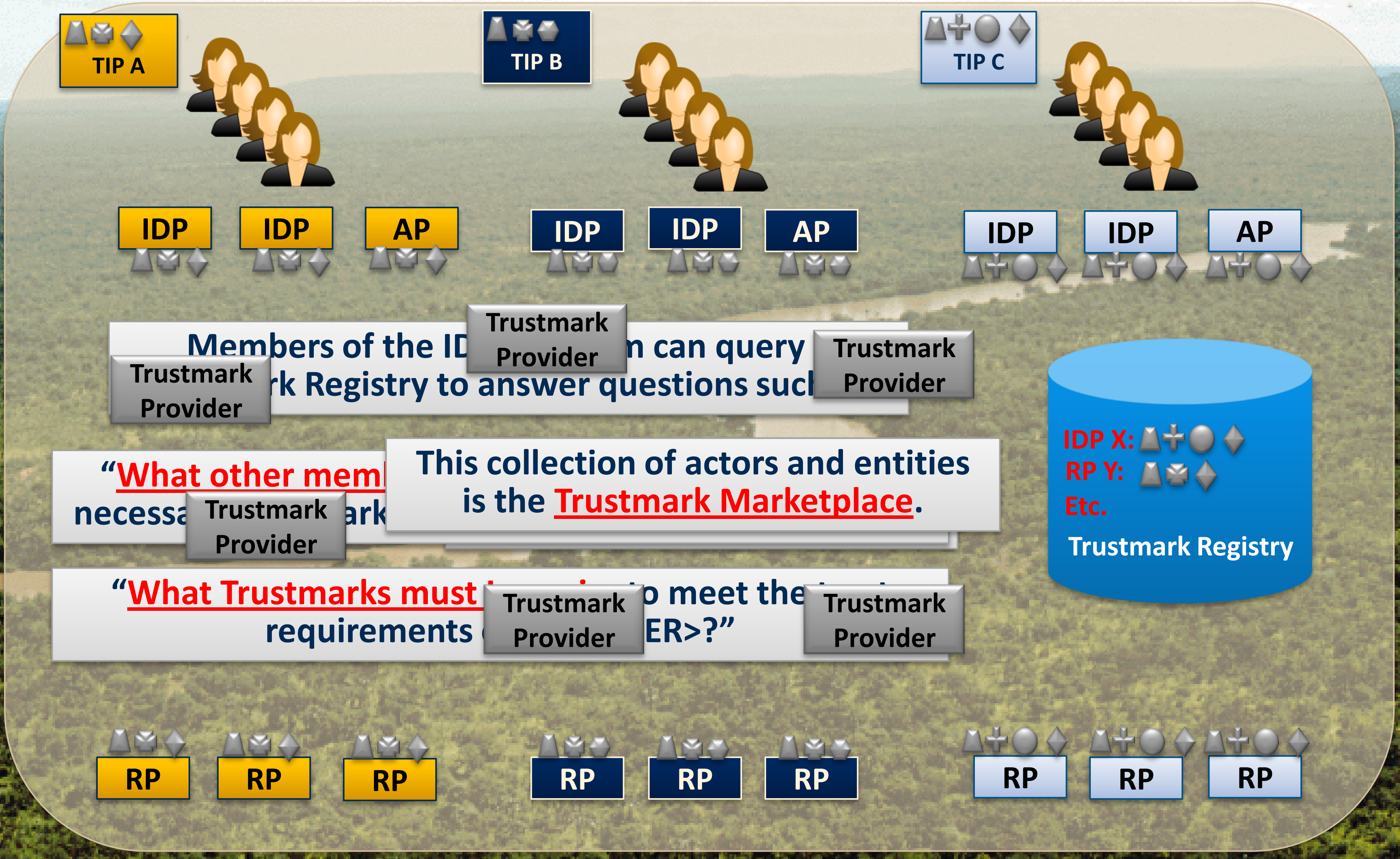
A Trustmark-Based ID Ecosystem



Then eac the n acquire TIP.

Some Trustmark Providers may specialize in issuing one particular Trustmark. Others may offer many Trustmarks.

A Trustmark-Based ID Ecosystem



Members of the ID n can query rk Registry to answer questions suc

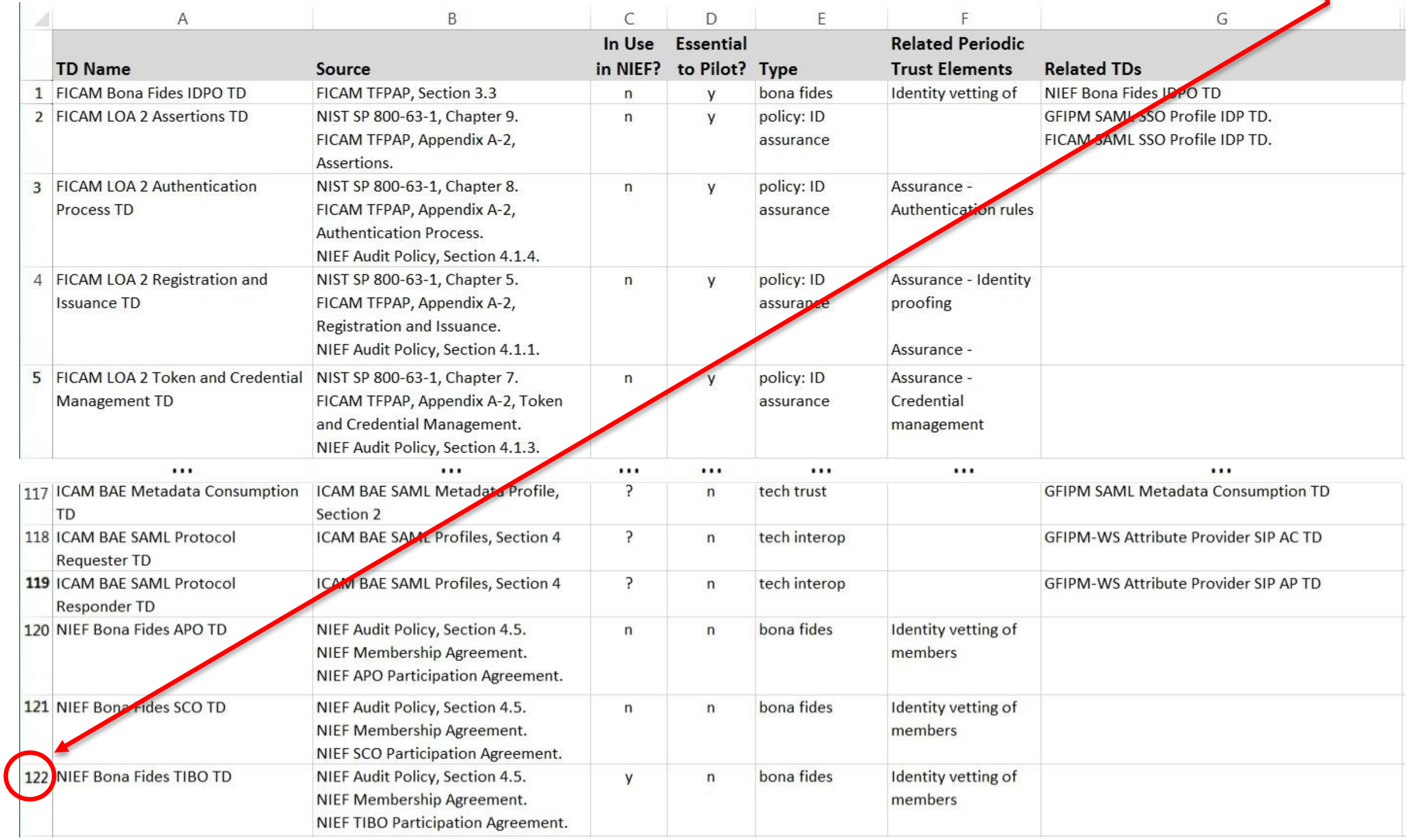
“What other mem necessa ark

This collection of actors and entities is the Trustmark Marketplace.

“What Trustmarks must o meet the requirements ER>?”

Initial Trustmark Analysis

- Expanded from a handful to over 120 trustmarks



	A	B	C	D	E	F	G
	TD Name	Source	In Use in NIEF?	Essential to Pilot?	Type	Related Periodic Trust Elements	Related TDs
1	FICAM Bona Fides IDPO TD	FICAM TFPAP, Section 3.3	n	y	bona fides	Identity vetting of	NIEF Bona Fides IDPO TD
2	FICAM LOA 2 Assertions TD	NIST SP 800-63-1, Chapter 9. FICAM TFPAP, Appendix A-2, Assertions.	n	y	policy: ID assurance		GFIPM SAML SSO Profile IDP TD. FICAM SAML SSO Profile IDP TD.
3	FICAM LOA 2 Authentication Process TD	NIST SP 800-63-1, Chapter 8. FICAM TFPAP, Appendix A-2, Authentication Process. NIEF Audit Policy, Section 4.1.4.	n	y	policy: ID assurance	Assurance - Authentication rules	
4	FICAM LOA 2 Registration and Issuance TD	NIST SP 800-63-1, Chapter 5. FICAM TFPAP, Appendix A-2, Registration and Issuance. NIEF Audit Policy, Section 4.1.1.	n	y	policy: ID assurance	Assurance - Identity proofing Assurance -	
5	FICAM LOA 2 Token and Credential Management TD	NIST SP 800-63-1, Chapter 7. FICAM TFPAP, Appendix A-2, Token and Credential Management. NIEF Audit Policy, Section 4.1.3.	n	y	policy: ID assurance	Assurance - Credential management	
	…	…	…	…	…	…	…
117	ICAM BAE Metadata Consumption TD	ICAM BAE SAML Metadata Profile, Section 2	?	n	tech trust		GFIPM SAML Metadata Consumption TD
118	ICAM BAE SAML Protocol Requester TD	ICAM BAE SAML Profiles, Section 4	?	n	tech interop		GFIPM-WS Attribute Provider SIP AC TD
119	ICAM BAE SAML Protocol Responder TD	ICAM BAE SAML Profiles, Section 4	?	n	tech interop		GFIPM-WS Attribute Provider SIP AP TD
120	NIEF Bona Fides APO TD	NIEF Audit Policy, Section 4.5. NIEF Membership Agreement. NIEF APO Participation Agreement.	n	n	bona fides	Identity vetting of members	
121	NIEF Bona Fides SCO TD	NIEF Audit Policy, Section 4.5. NIEF Membership Agreement. NIEF SCO Participation Agreement.	n	n	bona fides	Identity vetting of members	
122	NIEF Bona Fides TIBO TD	NIEF Audit Policy, Section 4.5. NIEF Membership Agreement. NIEF TIBO Participation Agreement.	y	n	bona fides	Identity vetting of members	

Trustmarks By Category

Georgia Tech Research Institute

Identity Assurance Policy
(10 Total, 10 Essential to Pilot)

Security Policy
(18 Total, 18 Essential to Pilot)

Privacy Policy
(23 Total, 15 Essential to Pilot)

Attribute Assurance Policy
(2 Total, 2 Essential to Pilot)

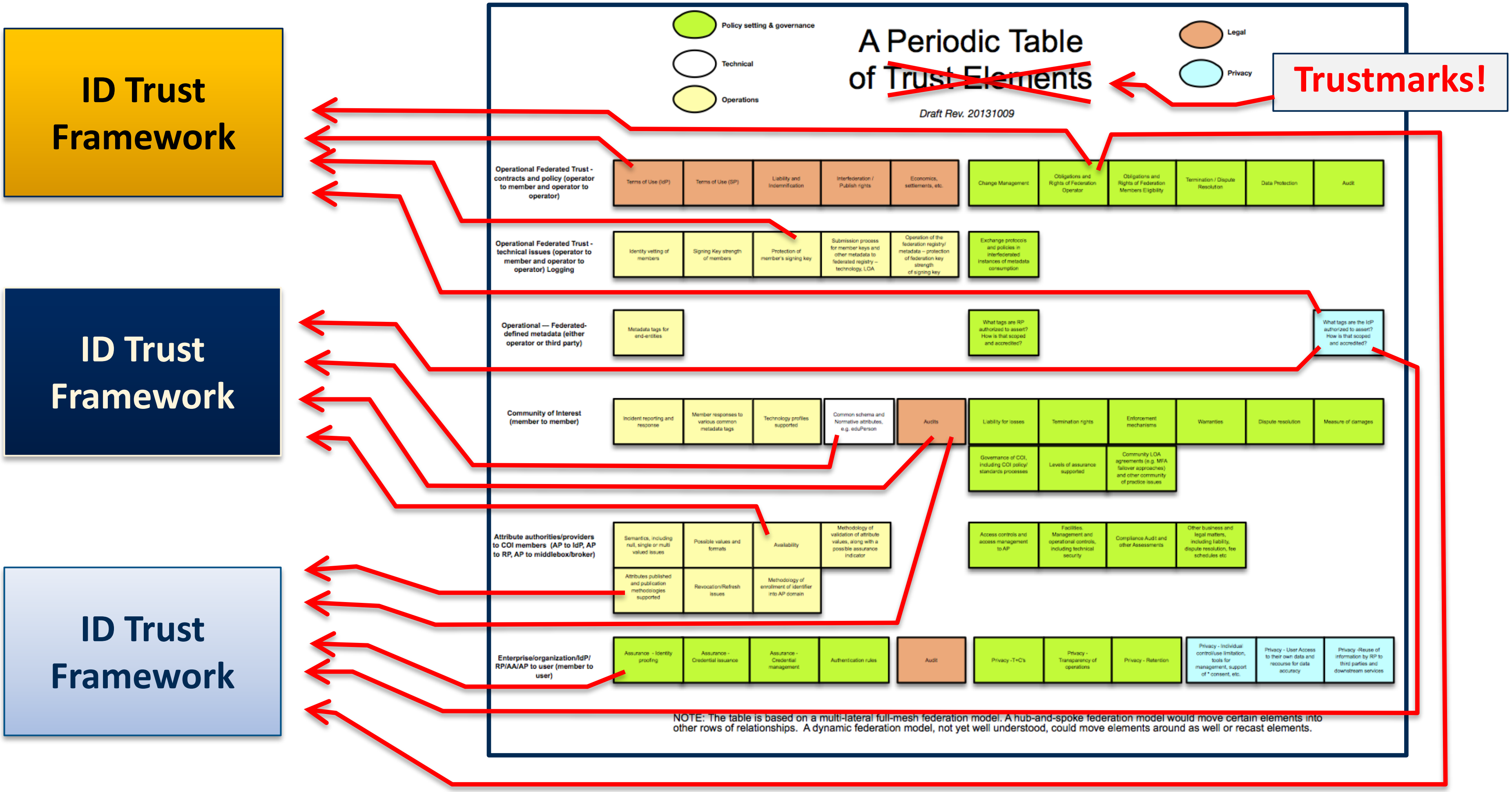
Technical Interoperability
(57 Total, 8 Essential to Pilot)

Organizational Integrity / Bona Fides
(6 Total, 3 Essential to Pilot)

Technical Trust
(4 Total, 3 Essential to Pilot)

Usability
(2 Total, 0 Essential to Pilot)

Another Component Perspective



ID Trust Framework

ID Trust Framework

ID Trust Framework

Trustmarks!

🟩 Policy setting & governance

○ Technical

🟨 Operations

🟧 Legal

🟦 Privacy

A Periodic Table of ~~Trust Elements~~

Draft Rev. 20131009

Operational Federated Trust - contracts and policy (operator to member and operator to operator)
- Terms of Use (IdP)
- Terms of Use (SP)
- Liability and Indemnification
- Interfederation / Publish rights
- Economics, settlements, etc.
- Change Management
- Obligations and Rights of Federation Operator
- Obligations and Rights of Federation Members Eligibility
- Termination / Dispute Resolution
- Data Protection
- Audit

Operational Federated Trust - technical issues (operator to member and operator to operator) Logging
- Identity vetting of members
- Signing Key strength of members
- Protection of member's signing key
- Submission process for member keys and other metadata to federated registry – technology, LOA
- Operation of the federation registry/ metadata – protection of federation key strength of signing key
- Exchange protocols and policies in interfederated instances of metadata consumption

Operational — Federated-defined metadata (either operator or third party)
- Metadata tags for end-entities
- What tags are RP authorized to assert? How is that scoped and accredited?
- What tags are the IdP authorized to assert? How is that scoped and accredited?

Community of Interest (member to member)
- Incident reporting and response
- Member responses to various common metadata tags
- Technology profiles supported
- Common schema and Normative attributes, e.g. eduPerson
- Audits
- Liability for losses
- Termination rights
- Enforcement mechanisms
- Warranties
- Dispute resolution
- Measure of damages
- Governance of COI, including COI policy/ standards processes
- Levels of assurance supported
- Community LOA agreements (e.g. MFA failover approaches) and other community of practice issues

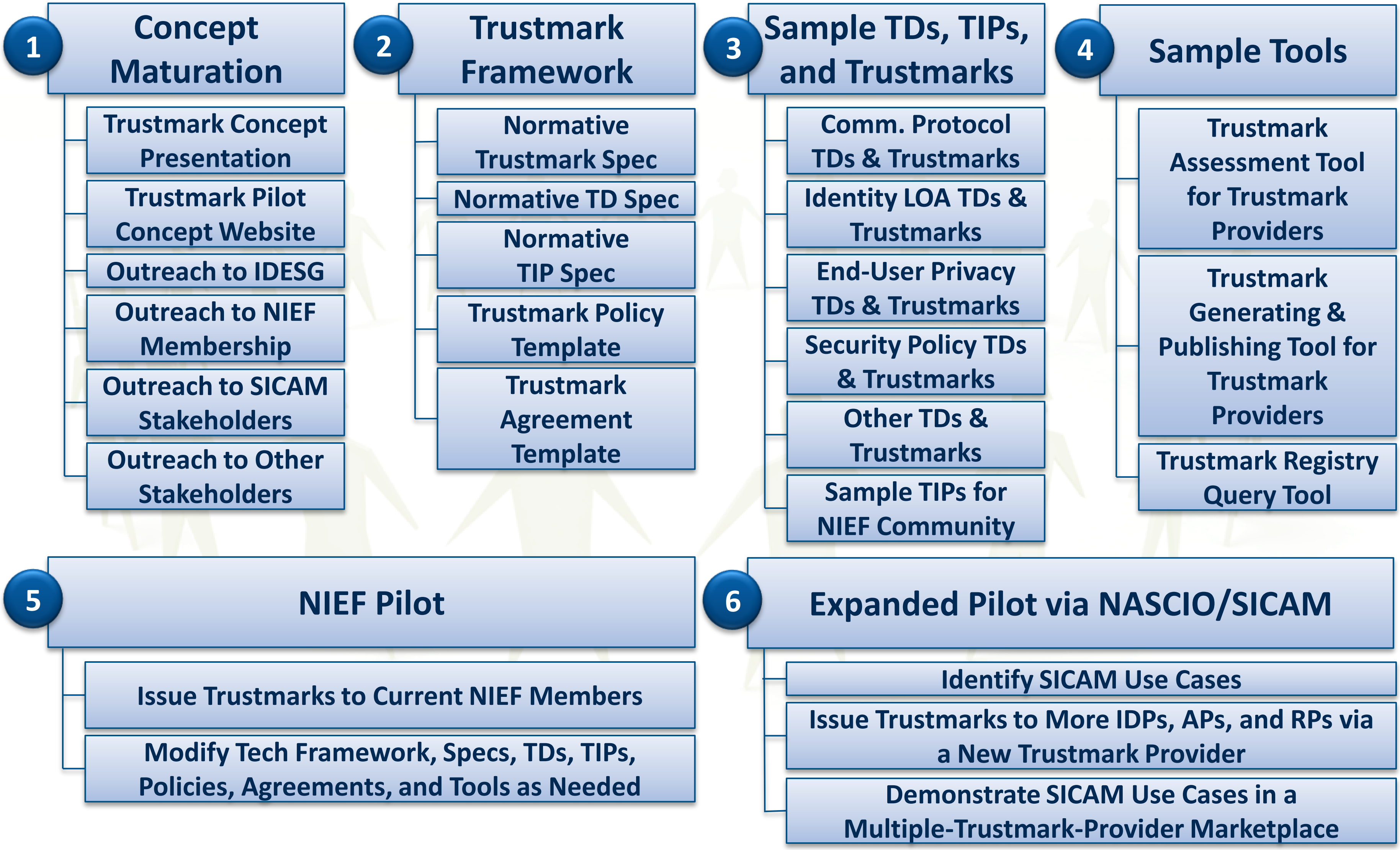
Attribute authorities/providers to COI members (AP to IdP, AP to RP, AP to middlebox/broker)
- Semantics, including null, single or multi valued issues
- Possible values and formats
- Availability
- Methodology of validation of attribute values, along with a possible assurance indicator
- Attributes published and publication methodologies supported
- Revocation/Refresh issues
- Methodology of enrollment of identifier into AP domain
- Access controls and access management to AP
- Facilities. Management and operational controls, including technical security
- Compliance Audit and other Assessments
- Other business and legal matters, including liability, dispute resolution, fee schedules etc

Enterprise/organization/IdP/ RP/AA/AP to user (member to user)
- Assurance - Identity proofing
- Assurance - Credential issuance
- Assurance - Credential management
- Authentication rules
- Audit
- Privacy -T+C's
- Privacy - Transparency of operations
- Privacy - Retention
- Privacy - Individual control/use limitation, tools for management, support of * consent, etc.
- Privacy - User Access to their own data and recourse for data accuracy
- Privacy -Reuse of information by RP to third parties and downstream services

NOTE: The table is based on a multi-lateral full-mesh federation model. A hub-and-spoke federation model would move certain elements into other rows of relationships. A dynamic federation model, not yet well understood, could move elements around as well or recast elements.

Source: Ken Klingenstein, Internet 2

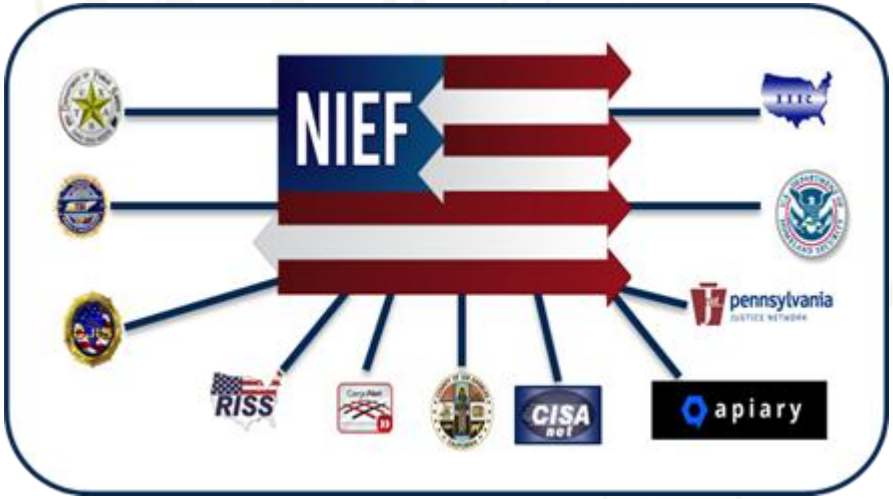
Scope of the NSTIC Trustmark Pilot



1. **Concept Maturation**
   - Trustmark Concept Presentation
   - Trustmark Pilot Concept Website
   - Outreach to IDESG
   - Outreach to NIEF Membership
   - Outreach to SICAM Stakeholders
   - Outreach to Other Stakeholders
2. **Trustmark Framework**
   - Normative Trustmark Spec
   - Normative TD Spec
   - Normative TIP Spec
   - Trustmark Policy Template
   - Trustmark Agreement Template
3. **Sample TDs, TIPs, and Trustmarks**
   - Comm. Protocol TDs & Trustmarks
   - Identity LOA TDs & Trustmarks
   - End-User Privacy TDs & Trustmarks
   - Security Policy TDs & Trustmarks
   - Other TDs & Trustmarks
   - Sample TIPs for NIEF Community
4. **Sample Tools**
   - Trustmark Assessment Tool for Trustmark Providers
   - Trustmark Generating & Publishing Tool for Trustmark Providers
   - Trustmark Registry Query Tool
5. **NIEF Pilot**
   - Issue Trustmarks to Current NIEF Members
   - Modify Tech Framework, Specs, TDs, TIPs, Policies, Agreements, and Tools as Needed
6. **Expanded Pilot via NASCIO/SICAM**
   - Identify SICAM Use Cases
   - Issue Trustmarks to More IDPs, APs, and RPs via a New Trustmark Provider
   - Demonstrate SICAM Use Cases in a Multiple-Trustmark-Provider Marketplace

The Trustmark Pilot Team

Georgia Tech Research Institute

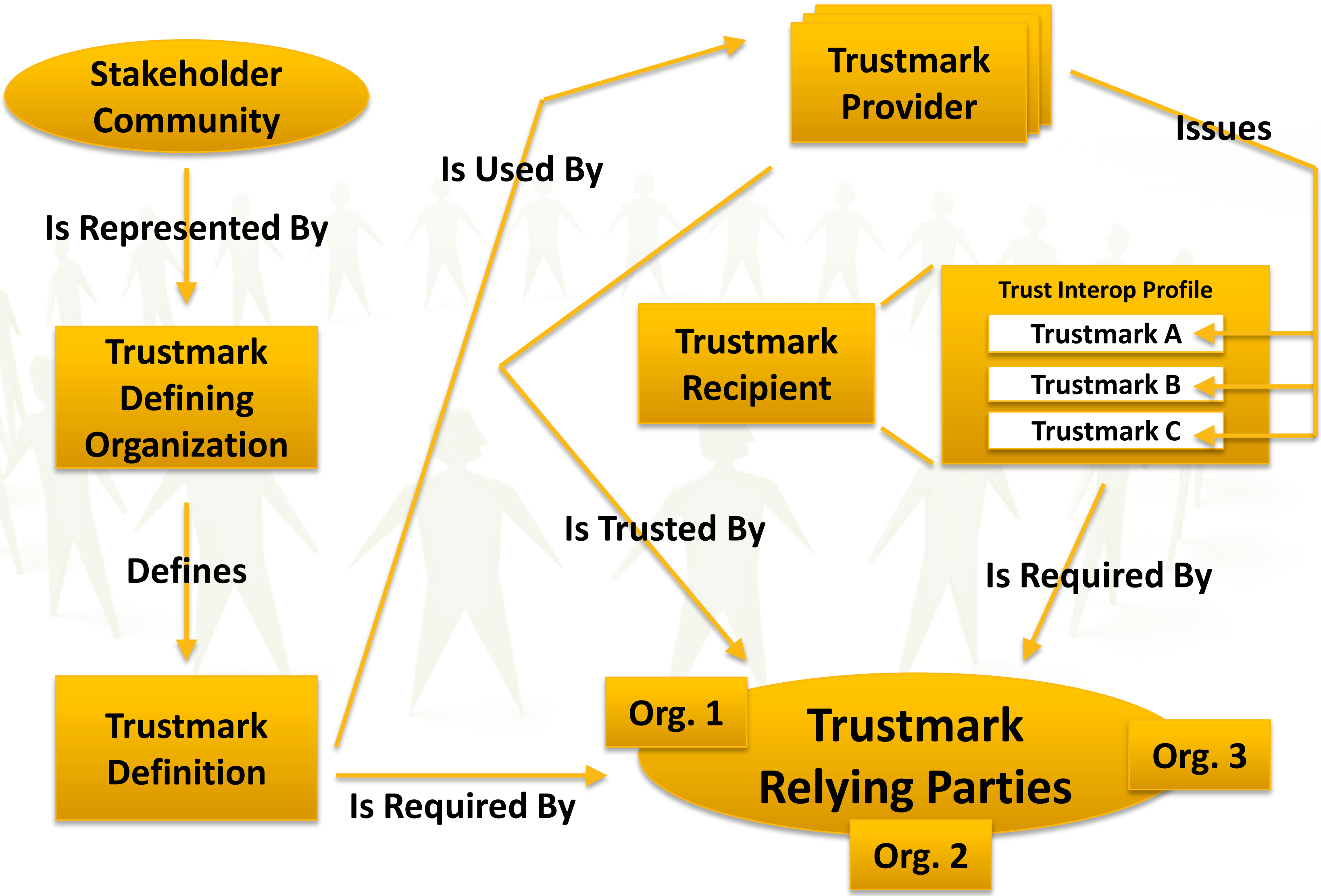


NASCIO
Representing Chief Information Officers of the States

Coming Soon……

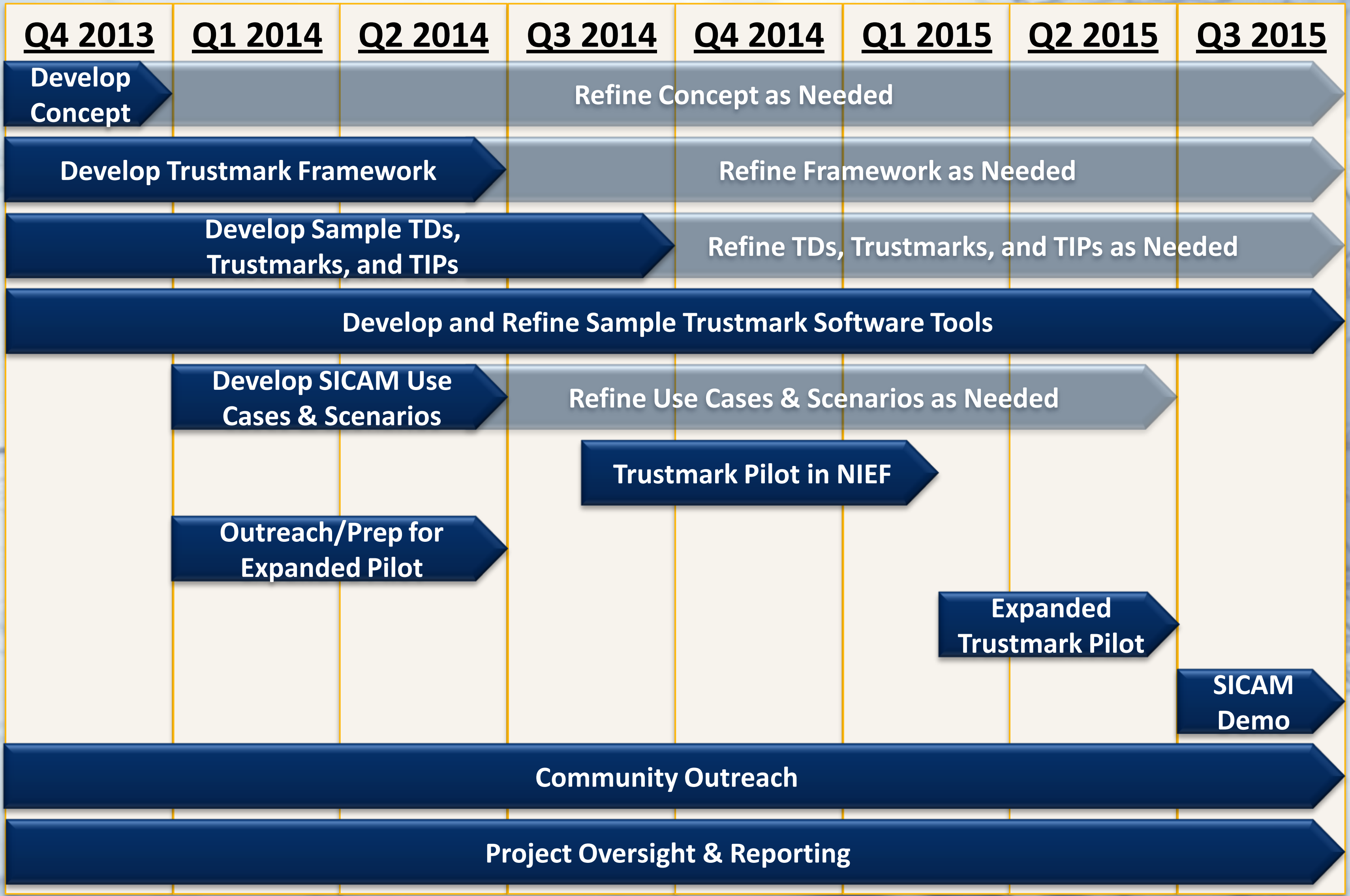
https://trustmark.gtri.gatech.edu

The Trustmark Concept Map



High-Level Project Plan & Timeline

Georgia Tech Research Institute



Q4 2013 | Q1 2014 | Q2 2014 | Q3 2014 | Q4 2014 | Q1 2015 | Q2 2015 | Q3 2015

Develop Concept

Refine Concept as Needed

Develop Trustmark Framework

Refine Framework as Needed

Develop Sample TDs, Trustmarks, and TIPs

Refine TDs, Trustmarks, and TIPs as Needed

Develop and Refine Sample Trustmark Software Tools

Develop SICAM Use Cases & Scenarios

Refine Use Cases & Scenarios as Needed

Trustmark Pilot in NIEF

Outreach/Prep for Expanded Pilot

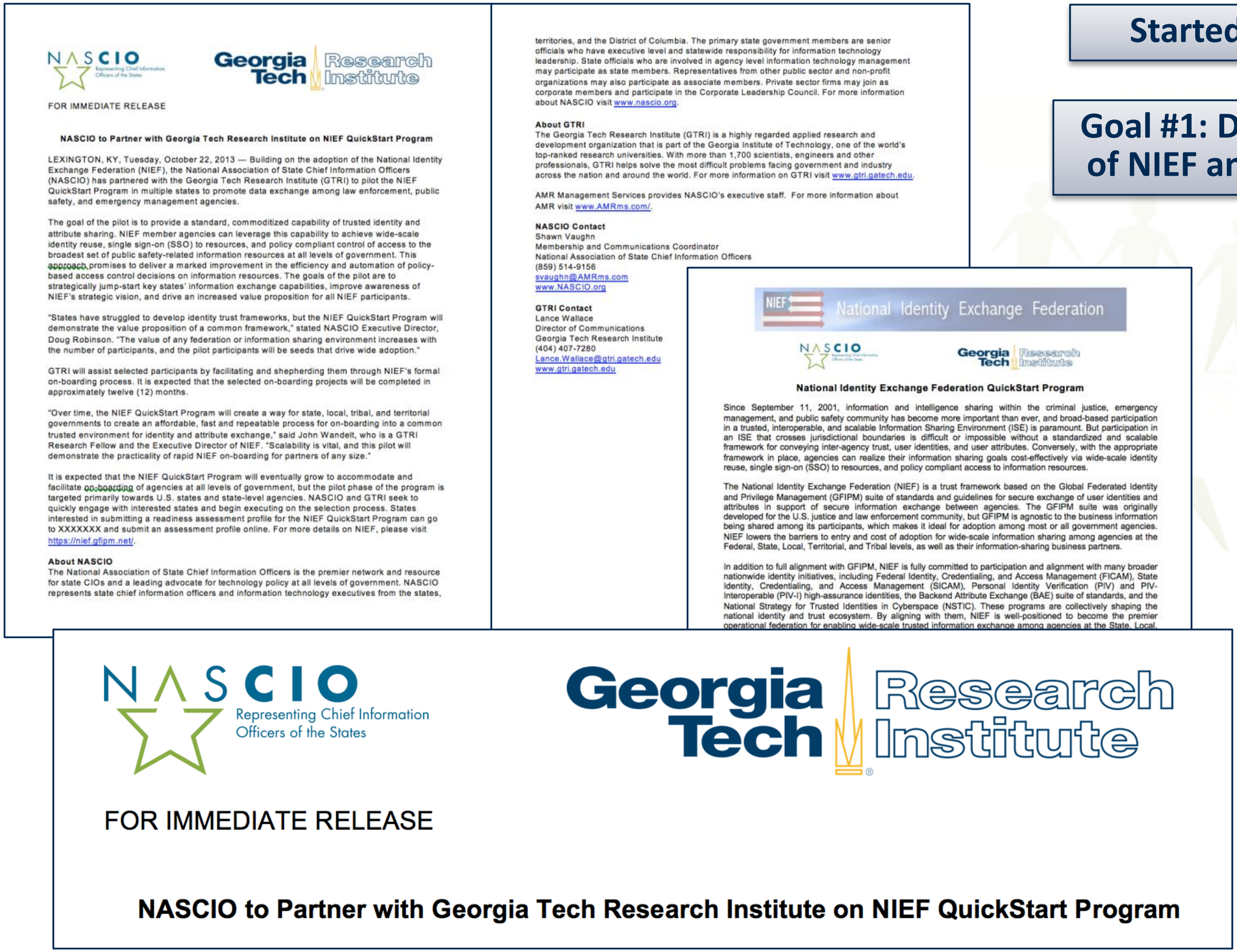
Expanded Trustmark Pilot

SICAM Demo

Community Outreach

Project Oversight & Reporting

The NIEF QuickStart Program



FOR IMMEDIATE RELEASE

NASCIO to Partner with Georgia Tech Research Institute on NIEF QuickStart Program

LEXINGTON, KY, Tuesday, October 22, 2013 — Building on the adoption of the National Identity Exchange Federation (NIEF), the National Association of State Chief Information Officers (NASCIO) has partnered with the Georgia Tech Research Institute (GTRI) to pilot the NIEF QuickStart Program in multiple states to promote data exchange among law enforcement, public safety, and emergency management agencies.

The goal of the pilot is to provide a standard, commoditized capability of trusted identity and attribute sharing. NIEF member agencies can leverage this capability to achieve wide-scale identity reuse, single sign-on (SSO) to resources, and policy compliant control of access to the broadest set of public safety-related information resources at all levels of government. This approach promises to deliver a marked improvement in the efficiency and automation of policy-based access control decisions on information resources. The goals of the pilot are to strategically jump-start key states' information exchange capabilities, improve awareness of NIEF's strategic vision, and drive an increased value proposition for all NIEF participants.

"States have struggled to develop identity trust frameworks, but the NIEF QuickStart Program will demonstrate the value proposition of a common framework," stated NASCIO Executive Director, Doug Robinson. "The value of any federation or information sharing environment increases with the number of participants, and the pilot participants will be seeds that drive wide adoption."

GTRI will assist selected participants by facilitating and shepherding them through NIEF's formal on-boarding process. It is expected that the selected on-boarding projects will be completed in approximately twelve (12) months.

"Over time, the NIEF QuickStart Program will create a way for state, local, tribal, and territorial governments to create an affordable, fast and repeatable process for on-boarding into a common trusted environment for identity and attribute exchange," said John Wandelt, who is a GTRI Research Fellow and the Executive Director of NIEF. "Scalability is vital, and this pilot will demonstrate the practicality of rapid NIEF on-boarding for partners of any size."

It is expected that the NIEF QuickStart Program will eventually grow to accommodate and facilitate on-boarding of agencies at all levels of government, but the pilot phase of the program is targeted primarily towards U.S. states and state-level agencies. NASCIO and GTRI seek to quickly engage with interested states and begin executing on the selection process. States interested in submitting a readiness assessment profile for the NIEF QuickStart Program can go to XXXXXXX and submit an assessment profile online. For more details on NIEF, please visit https://nief.gfipm.net/.

About NASCIO
The National Association of State Chief Information Officers is the premier network and resource for state CIOs and a leading advocate for technology policy at all levels of government. NASCIO represents state chief information officers and information technology executives from the states, territories, and the District of Columbia. The primary state government members are senior officials who have executive level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as state members. Representatives from other public sector and non-profit organizations may also participate as associate members. Private sector firms may join as corporate members and participate in the Corporate Leadership Council. For more information about NASCIO visit www.nascio.org.

About GTRI
The Georgia Tech Research Institute (GTRI) is a highly regarded applied research and development organization that is part of the Georgia Institute of Technology, one of the world's top-ranked research universities. With more than 1,700 scientists, engineers and other professionals, GTRI helps solve the most difficult problems facing government and industry across the nation and around the world. For more information on GTRI visit www.gtri.gatech.edu.

AMR Management Services provides NASCIO's executive staff. For more information about AMR visit www.AMRms.com/.

NASCIO Contact
Shawn Vaughn
Membership and Communications Coordinator
National Association of State Chief Information Officers
(859) 514-9156
svaughn@AMRms.com
www.NASCIO.org

GTRI Contact
Lance Wallace
Director of Communications
Georgia Tech Research Institute
(404) 407-7280
Lance.Wallace@gtri.gatech.edu
www.gtri.gatech.edu

National Identity Exchange Federation

National Identity Exchange Federation QuickStart Program

Since September 11, 2001, information and intelligence sharing within the criminal justice, emergency management, and public safety community has become more important than ever, and broad-based participation in a trusted, interoperable, and scalable Information Sharing Environment (ISE) is paramount. But participation in an ISE that crosses jurisdictional boundaries is difficult or impossible without a standardized and scalable framework for conveying inter-agency trust, user identities, and user attributes. Conversely, with the appropriate framework in place, agencies can realize their information sharing goals cost-effectively via wide-scale identity reuse, single sign-on (SSO) to resources, and policy compliant access to information resources.

The National Identity Exchange Federation (NIEF) is a trust framework based on the Global Federated Identity and Privilege Management (GFIPM) suite of standards and guidelines for secure exchange of user identities and attributes in support of secure information exchange between agencies. The GFIPM suite was originally developed for the U.S. justice and law enforcement community, but GFIPM is agnostic to the business information being shared among its participants, which makes it ideal for adoption among most or all government agencies. NIEF lowers the barriers to entry and cost of adoption for wide-scale information sharing among agencies at the Federal, State, Local, Territorial, and Tribal levels, as well as their information-sharing business partners.

In addition to full alignment with GFIPM, NIEF is fully committed to participation and alignment with many broader nationwide identity initiatives, including Federal Identity, Credentialing, and Access Management (FICAM), State Identity, Credentialing, and Access Management (SICAM), Personal Identity Verification (PIV) and PIV-Interoperable (PIV-I) high-assurance identities, the Backend Attribute Exchange (BAE) suite of standards, and the National Strategy for Trusted Identities in Cyberspace (NSTIC). These programs are collectively shaping the national identity and trust ecosystem. By aligning with them, NIEF is well-positioned to become the premier operational federation for enabling wide-scale trusted information exchange among agencies at the State, Local,

FOR IMMEDIATE RELEASE

NASCIO to Partner with Georgia Tech Research Institute on NIEF QuickStart Program

Started in October 2013

Goal #1: Drive wider adoption of NIEF among state agencies

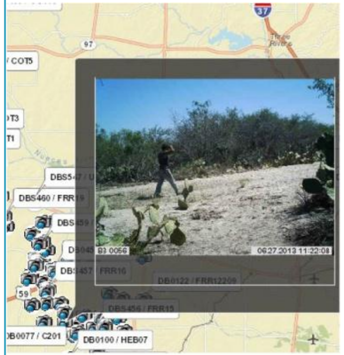
Goal #2: Streamline the NIEF onboarding process to drive more rapid NIEF adoption

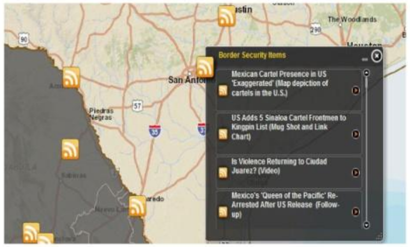
Timeframe: 12 Months

Objective: Identity at least 3 candidate agencies and onboard them into NIEF

Texas Department of Public Safety

TXMAP Web Mapping Application




Border Security Items

Mexican Cartel Presence in US 'Exaggerated' (Map depiction of cartels in the U.S.)

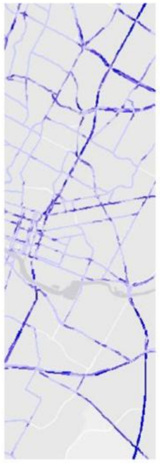
US Adds 5 Sinaloa Cartel Frontmen to Kingpin List (Mug Shot and Link Chart)

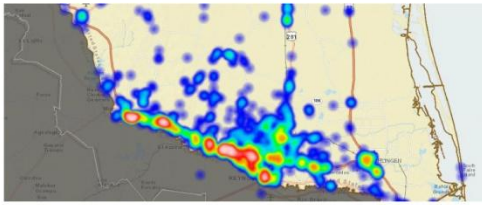
Is Violence Returning to Ciudad Juarez? (Video)

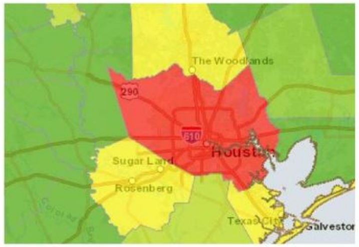
Mexico's 'Queen of the Pacific' Re-Arrested After US Release (Follow-up)

what is it?

The TXMAP application is a multi-faceted data mapping and reporting tool created by the Texas Department of Public Safety. TXMAP provides users access to a variety of data ranging from secure critical infrastructure and law enforcement data to public data such as registered sex offender home addresses.



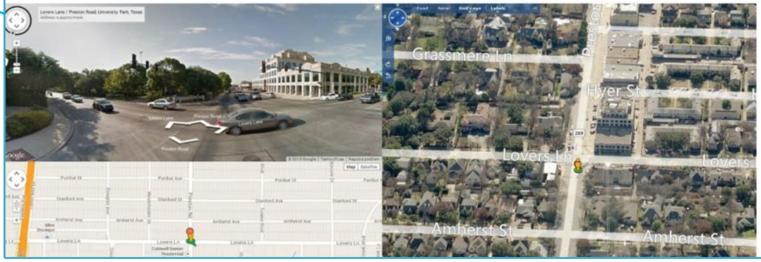




who is it for?

TXMAP would be a useful resource for:

- Law enforcement agencies
- Public safety organizations
- Emergency management groups



data samples

contacts

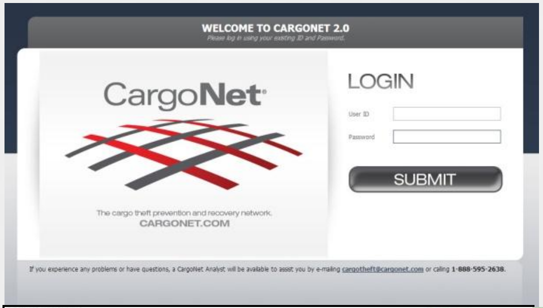
Paul Brown
Paul.brown@dps.texas.gov
P |512-424-7691

Shannon Wade
Shannon.wade@dps.texas.gov
P |512-424-7403

available Fall 2013

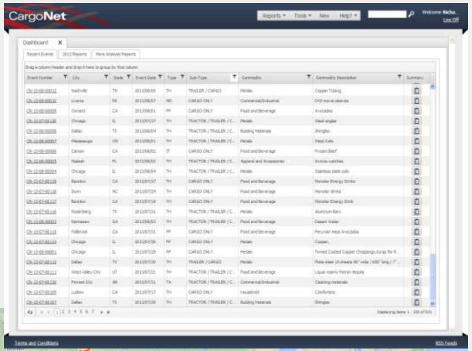
CargoNet

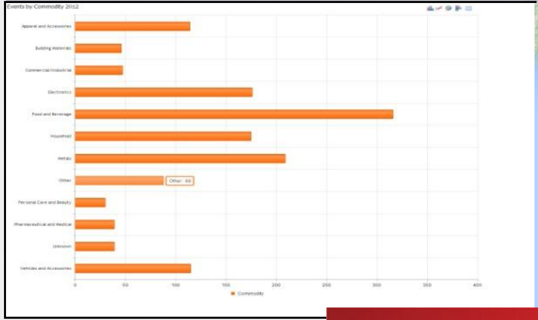
The Cargo Theft Prevention and Recovery Network

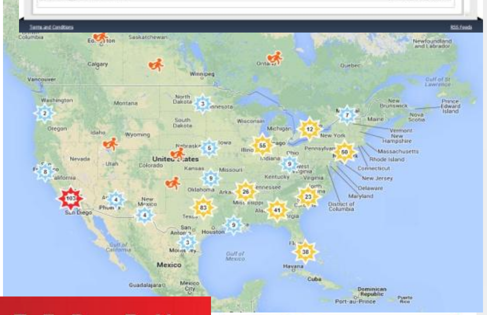

WELCOME TO CARGONET 2.0

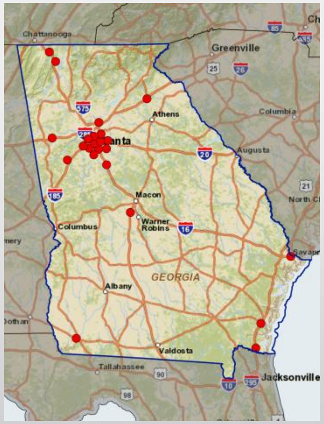
Please log in using your existing ID and Password.

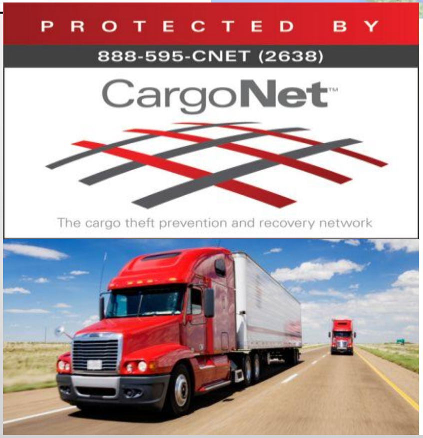
If you experience any problems or have questions, a CargoNet Analyst will be available to assist you by e-mailing cargotheft@cargonet.com or calling 1-888-595-2638.

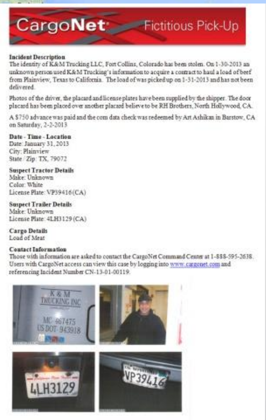



Events by Commodity 2012








CargoNet Fictitious Pick-Up

Incident Description
The identity of K&M Trucking LLC, Fort Collins, Colorado has been stolen. On 1-30-2013 an unknown person used K&M Trucking's information to acquire a contract to haul a load of beef from Plainview, Texas to California. The load of was picked up on 1-31-2013 and has not been delivered.

Photos of the driver, the placard and license plates have been supplied by the shipper. The door placard has been placed over another placard believe to be RH Brothers, North Hollywood, CA.

A $750 advance was paid and the com data check was redeemed by Art Ashikan in Barstow, CA on Saturday, 2-2-2013

Date - Time - Location
Date: January 31, 2013
City: Plainview
State / Zip: TX, 79072

Suspect Tractor Details
Make: Unknown
Color: White
License Plate: VP39416 (CA)

Suspect Trailer Details
Make: Unknown
License Plate: 4LH3129 (CA)

Cargo Details
Load of Meat

Contact Information
Those with information are asked to contact the CargoNet Command Center at 1-888-595-2638. Users with CargoNet access can view this case by logging into www.cargonet.com and referencing Incident Number CN-13-01-00119.

what is it?

CargoNet provides a multi-layered solution to the cargo theft problem. CargoNet helps prevent cargo theft and increases recovery rates by facilitating secure information sharing among theft victims, their business partners, and law enforcement. CargoNet offers **A 24 hours a day, 7 days a week** fusion center and cargo recovery network – staffed with security experts always available.

who is it for?

CargoNet is would be a useful resource for:

- Law Enforcement agencies
- Transportation industry
- Insurance industry
- Retail Industry

contact

Nigel DeFretias
CTO- Verisk Crime Analytics
W: 201.469.3939
ndefretias@verisk.com

status

Implementing SSO interface, beta testing anticipated in fall of 2013

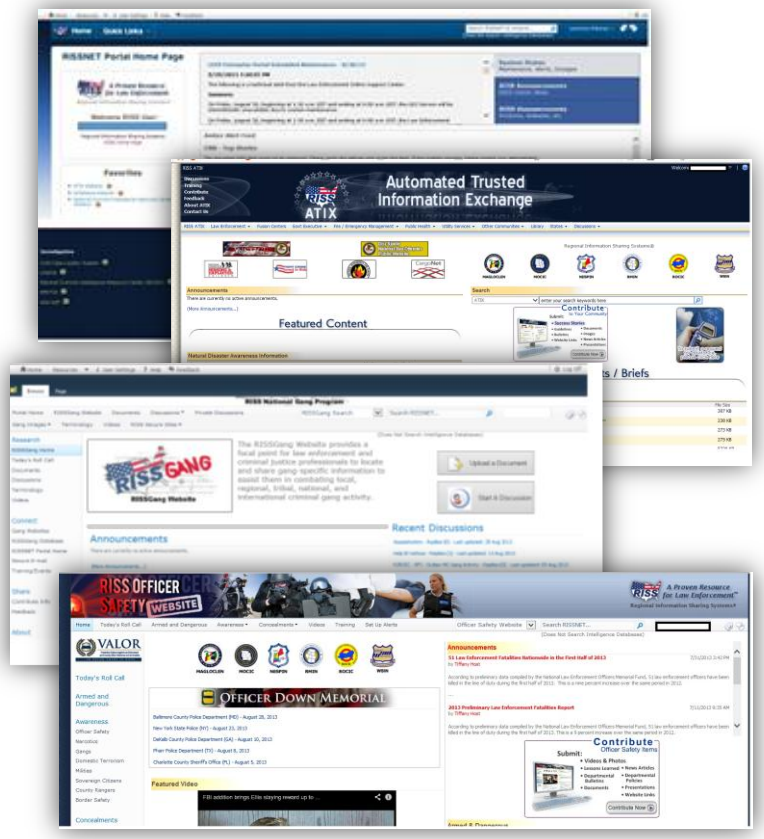
The cargo theft prevention and recovery network

CargoNet

The RISS Program is funded by Congress and administered by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice (DOJ).

The **RISSNET Portal currently** provides secure access to services and resources to more than 9,000 federal, state, local, and tribal law member enforcement agencies as well as public safety and Critical Infrastructure / Key Resource (CI / KR) communities. In addition, RISS' participation in NIEF allows RISS to provide different levels of authorization to NIEF users based upon user attributes.

- RISS Resources available to <u>all</u> federated partner users:
  - RISS ATIX Website - RISS TechPage - Intelink-U
- RISS Resources available only to Sworn Law Enforcement Officers (SLEO) or those acting for SLEO:
  - RISS National Gang Program (RISSGang) Web Site - RISS Officer Safety Website - Cold Case Locator System, National Criminal Intelligence Resource Center (NCIRC) - National Motor Vehicle Title Information System (NMVTIS) - Nationwide SAR Initiative (NSI) Search Tool (must have SAR account) - Federal law Enforcement Training Center (FLETC) Electronic Learning Portal (ELP)



Contact: Larry Maloney
(lmaloney@risstech.riss.net)

Tennessee

Meth & Pharmaceutical Task Force

Target Audience – Law Enforcement Use Only

TMIS (Tennessee Meth Intelligence System) is the State Repository for Meth Intelligence including Meth Lab Seizure Reporting, Pseudoephedrine Sales Tracking Information, and other intelligence. TMIS features computer generated and manual association development of suspects, cell phone analysis, custom searches, and automated notification of updates.

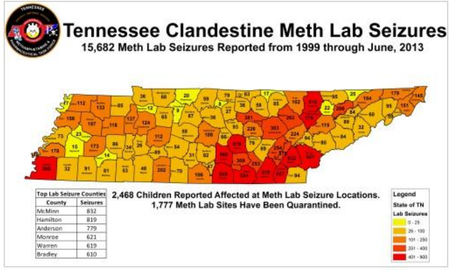
Status of Availability – Scheduled for Deployment Dec. 2013

Sponsoring Agency – Tennessee Bureau of Investigation

Contact Jim Derry at 423-752-1479 or jderry@rid-meth.org

If you cook it, we will come!

Tennessee Pain Clinics per County
284 Total Pain Clinics in Tennessee



Tennessee Clandestine Meth Lab Seizures
15,682 Meth Lab Seizures Reported from 1999 through June, 2013

Top Lab Seizure Counties	
County	Seizures
McMinn	832
Hamilton	819
Anderson	779
Monroe	621
Warren	619
Bradley	610

2,468 Children Reported Affected at Meth Lab Seizure Locations.
1,777 Meth Lab Sites Have Been Quarantined.

Homeland Security

HSIN | Homeland Security Information Network

HSIN is the nation's platform for sharing sensitive but unclassified information – enabling the Homeland Security Enterprise, its Federal, State, local, tribal, territorial, international and private sector partners, to meet their mission requirements through trusted information sharing.

HSIN Serves

- *Emergency Management*
- *Law Enforcement*
- *Public Health & Natural Resources*
- *Intelligence & Analysis*
- *Defense*
- *Emergency Services*

HSIN Offers

- *Incident and Event Collaboration*
- *Cross Community/Mission Information Sharing*
- *Operational Awareness & Coordination*
- *Real time Communication Tools*
- *Geospatial*

Contact
Tracy Hollis
Tracy.hollis@hwq.dhs.gov
202-357-6108

HSIN – DHS trusted information sharing and collaboration for mission partners

Apiary Threat Intelligence Framework

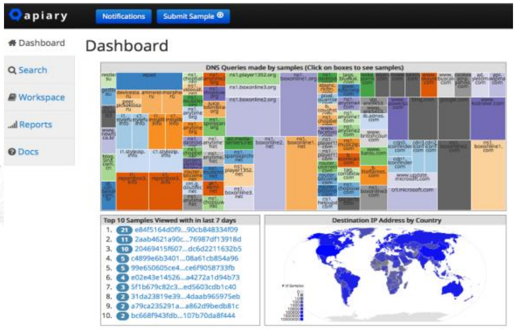
What is Apiary?

Apiary is an automated framework for malware analysis and threat intelligence. Members of our vetted community anonymously upload malware and benefit from the ongoing addition of in-depth malware correlation and behavior analysis. The results are delivered automatically within a secure sharing environment. The community is intended for analysts, investigators, or companies trying to protect their organization from malware.

Apiary processes approximately 150,000 malware samples per day allowing analysts to see the ‘big picture’ relationships and trends between malware samples. Our analysis techniques are backed by cutting edge research contributed by Apiary malware researchers as well as by members of the Apiary community. By automating the malware analysis process and sharing analysis data amongst a trusted community, organizations can confidently make security decisions.

Who uses Apiary

Apiary is currently being used in both the private and public sector. The community includes organizations from many industries including finance, oil and gas, utilities, retail, and more. Additionally, Apiary is used by local, state, and federal government organizations including law enforcement and education. The community is open, however all members are vetted before being allowed to access.



Top 10 Samples Viewed with in last 7 days

1. 21 e84f5164d0f9...90cb848334f09
2. 11 2aab4621a90c...76987df13918d
3. 10 20469415f607...dc6d2211632b5
4. 5 c4899e6b3401...08a61cb854a96
5. 5 99e650605ce4...ce6f9058733fb
6. 4 e02e43e14526...a4272a1d94b73
7. 3 5f1b679c82c3...ed5603cdb1c40
8. 2 31da23819e39...4daab965975eb
9. 2 a79ca235291a...a862d9bedb81c
10. 2 bc668f943fdb...107b70da8f444

Apiary and NIEF

Apiary will be integrated with NIEF by the end of 2013.

Points of Contact

For more information about Apiary, or to request to join the community, please email:

apiary-info@gtri.gatech.edu

LA County Criminal History

Target Audience – Law Enforcement , Probation and Prosecution

CCHRS is the LA County Criminal History System used by Investigators and Prosecutors for filing criminal cases within LA County. It contains over 12,000,000 subjects with their record of arrests, convictions, sentences, custody status, probation status, demographics and biometric identifiers. Over 44 local police agencies, LA Sheriff, LA District Attorney and LA Probation utilize CCHRS for their daily operations with 10,000+ transactions per day.

Status – Available Now (CCHRS-lite)

Sponsoring Agency – LA County Sheriff

Contact Rolf Embom at 562-403-6559 or rembom@isd.lacounty.gov

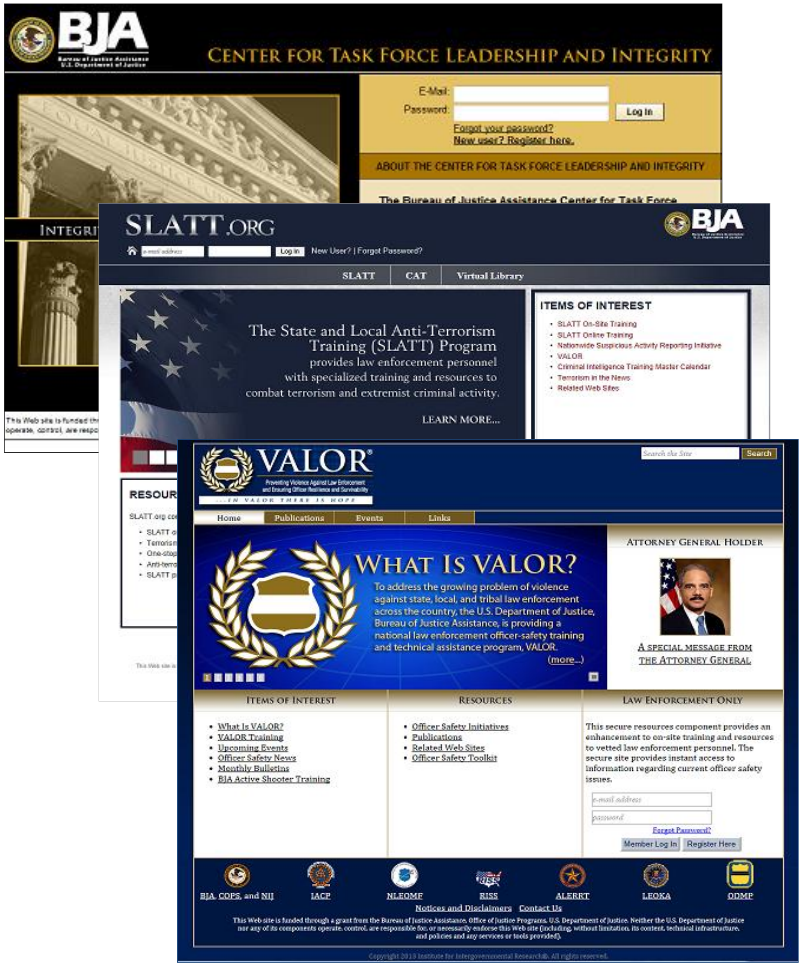
Brought to you by

Powered by

IIR
Institute for Intergovernmental Research®

Post Office Box 12729
Tallahassee, FL 32317
(850) 385-0600
www.iir.com

A trusted provider of superior training and specialized technical assistance services for law enforcement and public safety through innovative and effective solutions, the Institute for Intergovernmental Research (IIR) currently supports online training for multiple programs funded by the Bureau of Justice Assistance, including the Center for Task Force Leadership and Integrity (CTFLI), the State and Local Anti-Terrorism Training (SLATT®) Program, and VALOR, an officer-safety program. National Identify Exchange Federation (NIEF)-based credentials currently allow access to VALOR training and are expected to expand to other IIR-supported programs in the future.


BJA
Center for Task Force Leadership and Integrity
E-Mail:
Password:
Log In
Forgot your password?
New user? Register here.
About the Center for Task Force Leadership and Integrity
SLATT.ORG
BJA
Log In
New User? | Forgot Password?
SLATT
CAT
Virtual Library

The State and Local Anti-Terrorism Training (SLATT) Program provides law enforcement personnel with specialized training and resources to combat terrorism and extremist criminal activity.

LEARN MORE...

ITEMS OF INTEREST

- SLATT On-Site Training
- SLATT Online Training
- Nationwide Suspicious Activity Reporting Initiative
- VALOR
- Criminal Intelligence Training Master Calendar
- Terrorism in the News
- Related Web Sites

VALOR®
Preventing Violence Against Law Enforcement and Ensuring Officer Resilience and Survivability
...IN VALOR THERE IS HOPE
Search
Home
Publications
Events
Links
Attorney General Holder

WHAT IS VALOR?

To address the growing problem of violence against state, local, and tribal law enforcement across the country, the U.S. Department of Justice, Bureau of Justice Assistance, is providing a national law enforcement officer-safety training and technical assistance program, VALOR. (more...)

A special message from the Attorney General

ITEMS OF INTEREST

- What Is VALOR?
- VALOR Training
- Upcoming Events
- Officer Safety News
- Monthly Bulletins
- BJA Active Shooter Training

RESOURCES

- Officer Safety Initiatives
- Publications
- Related Web Sites
- Officer Safety Toolkit

LAW ENFORCEMENT ONLY

This secure resources component provides an enhancement to on-site training and resources to vetted law enforcement personnel. The secure site provides instant access to information regarding current officer safety issues.

This Web site is funded through a grant from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse this Web site (including, without limitation, its content, technical infrastructure, and policies and any services or tools provided).

Copyright 2013 Institute for Intergovernmental Research®. All rights reserved.

CTFLI www.cftli.org

The Center for Task Force Leadership and Integrity (CTFLI) is a restricted-access Web site providing training and resources that address the varying needs of law enforcement officers involved in task force operations. CTFLI assists state, local, and tribal law enforcement task force personnel in effectively combating multijurisdictional criminal organizations, while operating with integrity and accountability with regard to individuals' privacy, civil rights, and civil liberties and promoting officer safety.

SLATT www.slatt.org

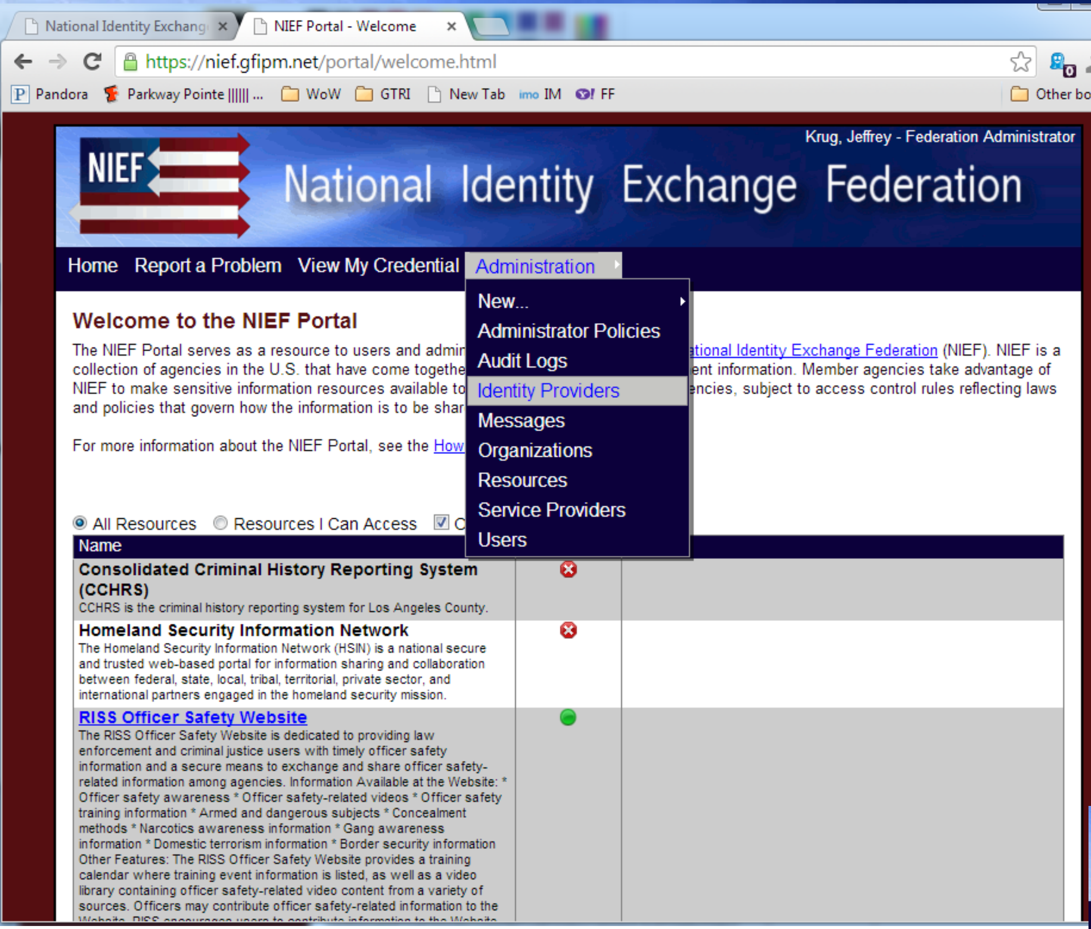
The SLATT Program provides specialized, critical multiagency anti-terrorism detection, investigation, and interdiction training and resources to our nation's state, local, and tribal law enforcement and prosecution authorities, who face the challenges presented by the terrorist/violent criminal extremist threat.

VALOR www.valorforblue.org

VALOR is an initiative designed to help prevent violence against law enforcement and ensure officer resilience and survivability following violent encounters during the course of their duties. Online training and resources are provided to state, local, and tribal law enforcement professionals through the valorforblue.org portal.

NIEF National Identity Exchange Federation

NIEF Portal



Welcome to the NIEF Portal

The NIEF Portal serves as a resource to users and admin ational Identity Exchange Federation (NIEF). NIEF is a collection of agencies in the U.S. that have come togethe ent information. Member agencies take advantage of NIEF to make sensitive information resources available to encies, subject to access control rules reflecting laws and policies that govern how the information is to be shar

For more information about the NIEF Portal, see the How

◉ All Resources ○ Resources I Can Access ☑ C

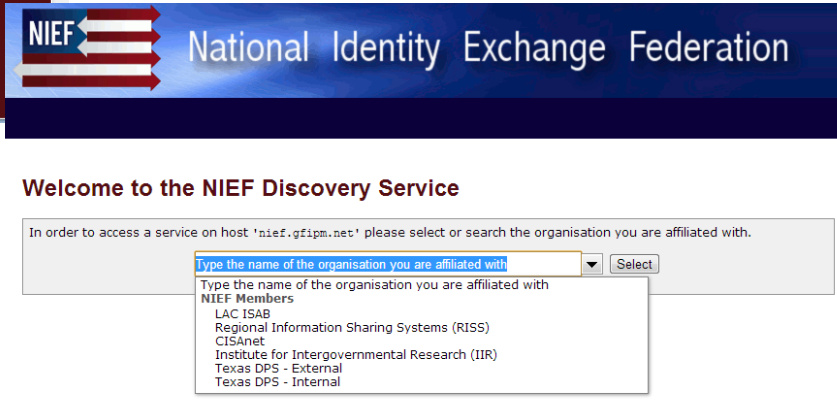
Name	
Consolidated Criminal History Reporting System (CCHRS) CCHRS is the criminal history reporting system for Los Angeles County.	☒
Homeland Security Information Network The Homeland Security Information Network (HSIN) is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.	☒
RISS Officer Safety Website The RISS Officer Safety Website is dedicated to providing law enforcement and criminal justice users with timely officer safety information and a secure means to exchange and share officer safety-related information among agencies. Information Available at the Website: * Officer safety awareness * Officer safety-related videos * Officer safety training information * Armed and dangerous subjects * Concealment methods * Narcotics awareness information * Gang awareness information * Domestic terrorism information * Border security information Other Features: The RISS Officer Safety Website provides a training calendar where training event information is listed, as well as a video library containing officer safety-related video content from a variety of sources. Officers may contribute officer safety-related information to the Website. RISS encourages users to contribute information to the Website	●

Organization Admins use the NIEF Portal to manage their organization’s details within NIEF.

NIEF Users discover available resources and whether their credential will grant them access.

Point of Contacts

John Wandelt: John.Wandelt@gtri.gatech.edu
Matthew Moyer: Matthew.Moyer@gtri.gatech.edu



Welcome to the NIEF Discovery Service

In order to access a service on host 'nief.gfipm.net' please select or search the organisation you are affiliated with.

Type the name of the organisation you are affiliated with

Type the name of the organisation you are affiliated with
NIEF Members
LAC ISAB
Regional Information Sharing Systems (RISS)
CISAnet
Institute for Intergovernmental Research (IIR)
Texas DPS - External
Texas DPS - Internal

Operated on behalf of the NIEF Center by GTRI

Georgia Tech Research Institute

Relationship of Programs to NIEF

- FICAM
  - NIEF Technical specs and policies are aligned with FICAM
  - NIEF has submitted formal application to be approved as a FICAM Trust Framework Provider @ LOA 2 and non-PKI LOA 3
- SICAM
  - SICAM currently only provides high-level guidance
  - Leverages FICAM and FICAM TFP initiatives
  - NIEF working with NASCIO to further mature SICAM through NIEF Quick Start program and NIEF NSTIC pilots
- NSTIC
  - Scope is broader than FICAM but leverages FICAM
  - NIEF selected by NIST to be a NSTIC pilot to demonstrate Scalable Trust and Interoperability through a Trustmark Marketplace
- BAE
  - NIEF piloted first operational BAE implementation in partnership with GSA, PM-ISE, TX DPS, RISS, IIR
  - NIEF has adopted BAE profile for Attribute Providers
- PIV/PIV-I
  - Under the sponsorship of DHS S&T and in partnership with JHAPL, GTRI to develop a proof of concept Gateway between the PIV-I community and NIEF
  - Also Leverages the BAE to collect additional attributes not on the PIV-I card